KECS-CR-10-40

XSmart e-Passport V1.1 인증보고서

인증번호 : KECS-ISIS-0253-2010

2010년 7월

IT보안인증사무국

제·개정 이력 현황

개정 번호	제·개정일	개정쪽	제·개정내용
00	2010. 7. 22	-	최초 작성

본 문서는 (주)LG CNS의 XSmart e-Passport V1.1에 대한 인증보고서이다.

인증기관

IT보안인증사무국

평가기관

한국인터넷진흥원

목 차

1. 요약

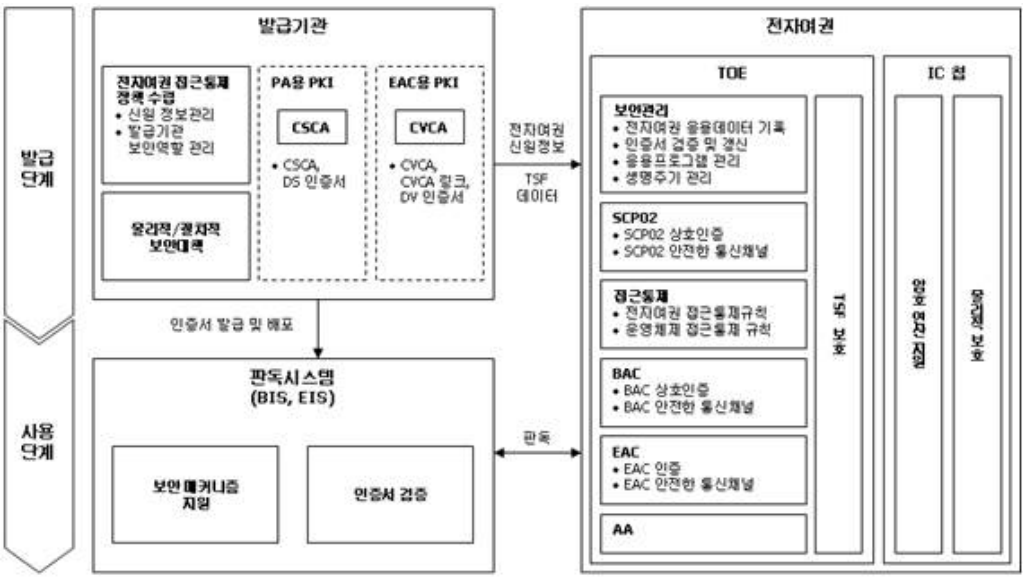
본 보고서는 XSmart e-Passport V1.1(이하 'TOE')에 대한 정보보호시스템 공통평가기준(2009년 9월 1일 고시)(이하 '공통평가기준'이 한다) EAL5+ 평가결과에 대한 인증기관의 인증결과를 서술한다. 본 보고서는 평가결과의 타당성 및 적합여부를 서술한다.

TOE에 대한 평가는 한국인터넷진흥원이 수행하였으며, 2010년 6월 25일에 평가가 완료되었다. 본 보고서의 내용은 한국인터넷진흥원에서 제출한 평가결과보고서의 내용에 기초하여 작성되었다. 평가는 제품이 공통평가기준 2부와 ADV_IMP.2가 추가된 EAL5 평가보증등급의 요구사항 3부를 만족함에 따라 "적합"한 것으로 평가하였다.

TOE는 하부 IC 칩 구성요소를 제외한 개방형 운영체제와 전자여권 응용프로그램으로 소프트웨어 형태로 구성된다. TOE는 개방형 운영체제를 기반으로 하여 전자여권의 MRZ 영역정보, 전자여권 신청인 기본정보, 전자여권 신청인 안면, 지문 등과 같은 바이오 정보, 인증 및 안전한 통신을 위한 암호키 등의 전자여권 응용데이터를 관리하며 발급기관 및 판독시스템을 인증하여 전자여권 사용자 데이터에 대한 접근 통제를 수행한다.

하부 IC칩은 CC EAL5+ 로 인증받은 삼성전자의 S3CC9LC 를 사용하고 있다. TOE가 기반으로 하는 IC 칩 구성요소에는 IC칩 하드웨어, IC칩 전용 펌웨어, 그리고 ECC 연산을 위한 암호연산 소프트웨어 라이브러리가 포함된다.

TOE는 IC 칩 하드웨어 및 안테나와 결합하여 전자여권을 구성하게 되며 IC 칩과 안테나는 TOE 범위에서 제외된다. TOE가 구동되는 운영환경은 [그림 1]과 같다.



[그림 1] TOE 운영환경

인증기관은 평가자의 평가활동 및 시험절차를 점검하고, 기술적인 문제점 및 평가절차에 대한 지침을 제공하고, 각 평가단위 및 평가결과보고서의 내용을 검토하였다. 인증기관은 평가결과가 평가제품이 보안목표명세서에 서술된 모든 보안기능 요구사항 및 보증요구사항을 만족함을 보증함을 확인하였다. 따라서, 인증기관은 평가자의 관찰사항, 평가결과가 정확하고 타당하다고 인증하였다.

인증 효력범위 : 본 인증결과보고서에 포함된 정보는 XSmart e-Passport V1.1이 대한민국 정부기관에 의한 사용 승인을 의미하지 않는다.

2. 식별정보

다음 [표 1]은 평가제품 식별을 위한 정보를 나타낸다.

[표 1] 평가대상제품 식별정보

평가지침	정보보호시스템 평가·인증 지침 (2009. 9. 1) 정보보호제품 평가인증 수행규정 (2010. 1. 1)
평가제품	XSmart e-Passport V1.1
보호프로파일	전자여권 보호프로파일 V2.1
보안목표명세서	XSmart e-Passport V1.1 보안목표명세서 V1.4
평가보고서	XSmart e-Passport V1.1 평가보고서, 발행버전 1.0 (2010. 6. 25)
적합여부 평가결과	공통평가기준 2부 적합 공통평가기준 3부 적합
평가기준	정보보호시스템 공통평가기준 V3.1 (2009. 9.1)
평가방법론	정보보호시스템 공통평가방법론 V3.1 (2009. 9.1)
평가신청인	(주)LG CNS
개발업체	(주)LG CNS
평가자	한국인터넷진흥원 공공정보보호단 공공서비스보호팀 현진수, 김일곤, 한정훈
인증담당자	IT보안인증사무국

3. 보안정책

평가제품은 아래와 같은 보안정책을 준수하여 운영된다.

P.국제적호환성

전자여권 발급기관은 발급된 전자여권의 보안메커니즘과 국외 입국 심사를 위한 판독시스템의 보안메커니즘 호환성을 보장해야 한다.

응용 시 주의사항 : 전자여권 규격 및 EAC 규격을 준수하여 국제적호환성을 보장하여야 한다.

P.보안메커니즘적용절차

TOE는 전자여권 발급기관의 전자여권 접근통제 정책에 위배되지 않도록 판독시스템 유형에 따른 보안메커니즘 적용순서를 보장하여야 한다.

응용 시 주의사항 : TOE는 판독시스템이 지원하는 보안메커니즘 종류에 따라 동작흐름이 달라진다. 기본 동작흐름은 EAC 규격의 2.1.1절에 서술된 표준 전자여권 판독절차(Standard ePassport Inspection Procedure)와 2.1.2 보안강화 전자여권 판독절차(Advanced ePassport Procedure)를 따른다.

P.응용프로그램탑재

전자여권 발급기관은 전자여권 IC칩에 탑재되는 응용프로그램이 TOE의 안전성에 영향을 미치지 않는지 확인한 후 탑재를 승인하여야 한다.

응용 시 주의사항 : 응용프로그램 탑재는 발급기관과 동등한 권한을 가진 기관만이 할 수 있다. 또한 전자여권 IC 칩에 탑재되어 설치된 전자여권 응용프로그램은 사용단계에서는 삭제될 수 없다.

P.전자여권발급기관

전자여권 발급기관은 발급 주체가 변경되지 않았음을 확인할 수 있도록 전자여권을 안전하게 발급하여야 하며 발급 이후 전자여권 IC 칩 내의 데이터가 정상적으로 동작함을 검증한 후 사용 단계로 넘겨야 한다. 발급기관은 TOE를 사용 단계로 전달하기 전에 쓰기 기능을 비활성화시켜야 한다. 또한 전자여권 발급기관은 운영체제 관리에 대한 접근통제 정책을 수립해야 한다.

응용 시 주의사항 : 발급기관 인증을 위한 보안메커니즘으로 'GP 규격'의 SCP02 보안메커니즘을 사용해야 한다.

P.전자여권접근통제

전자여권 발급기관 및 TOE는 전자여권 응용 데이터를 보호하기 위하여 전자여권 접근통제 정책을 수립하여야 한다. 또한, TOE는 사용자 역할을 규정해야 한다.

응용 시 주의사항 : TOE는 전자여권 규격 및 EAC 규격에 따라 다음과 같이 접근통제 정책을 수립해야 한다.

		객체목록	객체									
			전자여권 신청인 기본정보		전자여권 신청인 바이오정보		전자여권 인증정보		EF.CVCA		EF.COM	
주체목록			읽기 권한	쓰기 권한	읽기 권한	쓰기 권한	읽기 권한	쓰기 권한	읽기 권한	쓰기 권한	읽기 권한	쓰기 권한
주체	판독시스템	BAC권한	허용	거부	거부	거부	허용	거부	허용	거부	허용	거부
		EAC권한	허용	거부	허용	거부	허용	거부	허용	거부	허용	거부
	발급기관	발급권한	거부	허용	거부	허용	거부	허용	거부	허용	거부	허용

P. PKI

전자여권 발급국가는 여권전자서명체계에 따라 PA용 PKI 및 EAC용 PKI를 구축하여 인증업무준칙에 따라 전자서명키를 안전하게 생성·관리하고 인증서 생성·발급·운영·폐지 등 인증업무를 수행한다.

또한, 전자여권 발급국가는 인증서 유효기간 관리정책에 따라 인증서를 갱신하여 검증국가 및 판독시스템으로 안전하게 배포한다. 판독시스템은 TOE에 저장된 EF.CVCA로부터 정보를 얻은 후 EAC-TA에서 TOE에게 CVCA 링크인증서, DV 인증서, IS 인증서를 제공하면 TOE는 인증서유효성을 검증하여 인증서를 내부적으로 갱신하여야 한다.

P.RF통신 범위

전자여권 IC 칩과 판독시스템의 RF 통신거리는 5cm이내여야 하며 전자여권의 IC 칩 부착 면이 펼쳐지지 않은 경우에는 RF 통신채널이 형성되지 않아야 한다.

4. 가정사항 및 범위

4.1 가정사항

평가제품은 아래와 같은 가정사항을 준수하여 설치 및 운용되어야 한다.

A.인증서검증

BIS, EIS 등 판독시스템은 TOE에 기록된 전자여권 신원정보의 위변조를 검증하기 위해 PA용 인증서 체인(CSCA 인증서→DS 인증서)의 유효성을 검증한 후 SOD를 검증한다. 이를 위해, 주기적으로 DS 인증서 및 CRL을 검증해야 한다.

EIS는 IS 인증서에 대응되는 전자서명생성키를 안전하게 가지고 있어야 하며 EAC-TA 과정에서 TOE에게 CVCA 링크인증서, DV 인증서, IS 인증서를 제공하여야 한다.

응용 시 주의사항 : 판독시스템은 판독시스템의 PA용 인증서 체인 검증을 위해 주기적으로 ICAO-PKD에 접속하여 CSCA 인증서를 다운로드하여야 한다.

A.판독시스템

판독시스템은 출입국 자에 대한 전자여권 검증정책에 따라 전자여권 규격 및 EAC 규격에 따라 PA, AA, BAC, EAC 등 보안메커니즘을 구현해야 한다.

또한, BIS 및 EIS는 BAC 세션키, EAC 세션키, 세션정보 등 TOE와 통신에 사용된 정보를 세션이 종료된 이후에 모두 안전하게 파기해야 한다.

응용 시 주의사항 : TOE는 BAC 상호인증을 성공하지 못한 판독시스템에게는 EF.SOD 접근을 요청하는 경우 거부한다.

BIS는 BAC 및 PA 보안메커니즘을 지원하므로 BAC 인증키를 이용한 BAC 상호인증이 성공하면 전자여권 신청인 기본정보 및 인증정보에 대한 읽기권한을 얻고 BAC 세션 키를 이용한 BAC 안전한 통신채널을 형성함으로써 모든 송 수신데이터에 대해 비밀성 및 무결성을 보장한다. BIS는 BAC 수행 이후 PA를 수행하여 SOD를 검증하고 전자여권 신청인 기본정보 및 인증정보의 해시값 계산 및 비교를 통해 전자여권 신청인 기본정보 및 인증정보의 위변조를 검증한다.

EIS는 BAC, EAC 및 PA 보안메커니즘을 지원하므로 전자여권 신청인 기본정보 및 인증정보에 대한 읽기권한뿐만 아니라 전자여권 신청인 바이오정보에 대한 읽기 권한을 갖는다. EIS는 BAC 상호인증 및 BAC 안전한 통신채널 형성이 성공되면 TOE의 진위성을 검증하기 위해 BAC 수행과정에서 읽은 EAC 칩 인증 공개키를 이용하여 EAC-CA 과정을 수행하고 EAC 칩 인증 공개키를 검증하기 위해 PA를 수행한다. EAC-CA 수행을 성공하면 BAC 안전한 통신채널을 종료하고 EAC 세션 키를 이용한 EAC 안전한 통신채널을 다시 시작하여 TOE가 판독시스템을 인증하는 EAC-TA 과정을 수행한다. EAC-TA를 성공하면 전자여권 신청인 바이오정보 읽기권한을 획득한 것이므로 TOE로부터 전자여권 신청인 바이오정보를 제공받는다.

BIS 및 EIS는 추가적으로 AA 보안메커니즘을 구현할 수 있고, 이를 통해 TOE가 제공하는 전자서명을 EF.DG15의 AA 전자서명 검증키를 이용하여 검증하여 TOE의 복제여부를 검증한다.

A.IC칩

TOE의 하부 플랫폼인 IC 칩은 TOE의 보안기능성을 지원하기 위해 난수 생성 및 암호 연산을 제공하며 정상동작 범위를 벗어나는 경우를 탐지하고, 역공학 분석 및 탐침(Probing) 등을 이용한 물리적 공격으로부터 TOE를 보호하기 위한 물리적 보호 기능을 제공한다

응용 시 주의사항 : TOE의 안전성을 보장하기 위해 IC 칩은 CCRA EAL5+의 인증제품인 S3CC9LC이다. IC 칩이 지원하는 암호 연산은 IC칩의 암호 전용 프로세서 및 IC 칩에 탑재되는 암호 라이브러리에서 제공된다.

A.MRZ엔트로피

BAC 인증키 Seed 값은 BAC 인증키의 안전성을 보장할 수 있는 정도의 MRZ 엔트로피를 갖는다.

응용 시 주의사항 : 중간수준의 위협원으로부터 내성을 가지기 위해 MRZ 중 BAC 인증키 Seed 값으로 사용되는 여권번호, 생년월일, 여권유효기간, Check Digit의 엔트로피는 최소 56bit 이상이다.

4.2 위협 대응범위

전자여권은 물리적으로 통제된 장치 없이 개인이 소지하여 사용하므로, 논리적인 위협과 함께 물리적인 위협도 발생한다.

위협원은 TOE 외부에서 물리적 또는 논리적 방법을 사용하여 TOE가 보호하고자 하는 자산에 불법적인 접근을 시도하는 외부 실체이다.

본 인증결과보고서에서는 가정사항 A.IC칩에 따라 TOE를 보호하기 위해 IC칩이 물리적 보호 기능을 제공하므로 높은 수준의 위협원에 의한 IC칩 자체의 물리적 위협은 고려하지 않지만, 그럼에도 불구하고 논리적 방법을 통한 높은 수준의 공격 가능성이 높음을 무시할 수 있다.

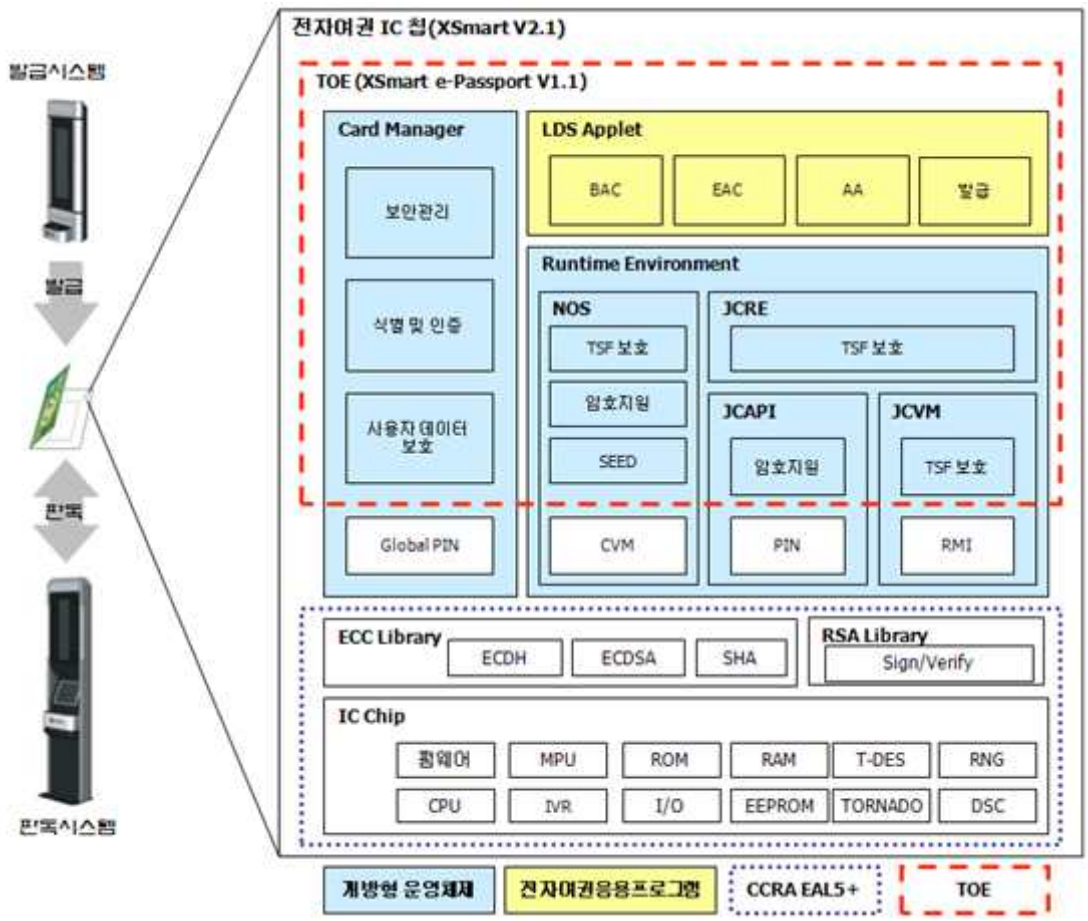
따라서 TOE에 대한 위협원은 높은 수준의 전문지식, 자원, 동기를 가지고, 공격자가 악용 가능한 취약성을 발견할 가능성은 높음이다.

5. 제품정보

전자여권은 여권책자와 여권책자 표지에 내장되는 전자여권 IC 칩 및 안테나를 의미한다. 전자여권 IC 칩은 전자여권 응용프로그램, 실행환경과 카드 매니저로 구성되는 개방형 운영체제, 그리고 IC 칩 구성요소인 IC칩 하드웨어, 펌웨어, ECC/RSA 암호연산 라이브러리를 포함한다.

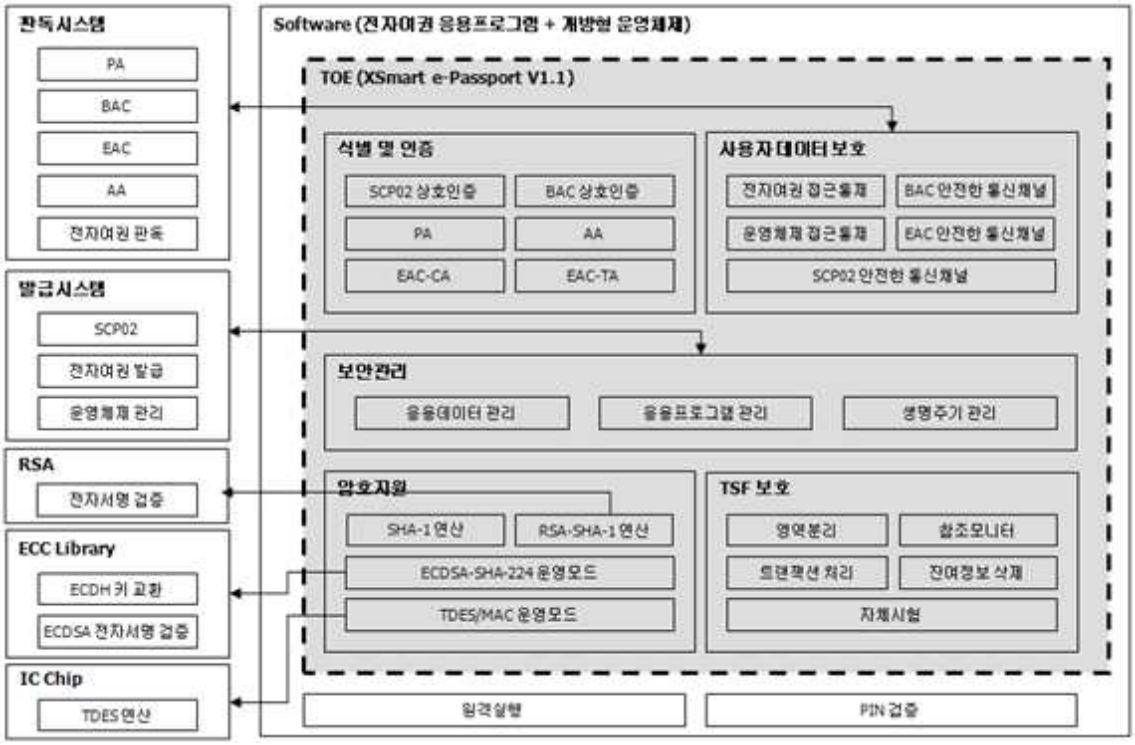
TOE는 전자여권 IC칩 내에 탑재된 개방형 운영체제와 전자여권 응용프로그램으로 정의하며 IC칩 구성요소인 IC칩 하드웨어, 펌웨어, ECC/RSA 암호연산 라이브러리는 TOE 범위에서 제외한다.

TOE는 삼성전자의 S3CC9LC IC 칩위에 탑재되며 물리적 범위는 [그림 2]와 같다.



[그림 2] TOE 물리적 범위

TOE의 논리적 범위는 [그림 3]과 같다.



[그림 3] TOE 논리적 범위

TOE는 식별 및 인증, 사용자 데이터 보호, 보안관리, TSF 보호, 암호지원의 보안기능을 제공한다.

· 식별 및 인증

TOE는 식별 및 인증을 위한 수단으로 SCP02 상호인증, BAC 상호인증, EAC-CA, EAC-TA, PA 및 AA를 제공한다.

<SCP02 상호인증>

SCP02(Secure Channel Protocol 02)는 TOE에 전자여권 신청인 신상정보 및 TSF 데이터에 대한 쓰기, 추가, 갱신 권한을 가진 발급기관을 인증하는 보안메커니즘으로 SCP02 상호인증 및 안전한 통신채널을 포함한다. TOE와 발급기관은 발급기관 인증정보와 SC(Sequence Counter)를 이용하여 SCP02 세션 키를 생성한 후, 상호 교환한 난수에 대한 MAC 값을 TOE와 발급기관이 상호 검증하는 방법으로 상호 인증을 수행한다. SCP02 상호인증이 실패하면 세션을 종료하고 성공하면 TOE는 SCP02 세션 키를 이용하여 안전한 통신채널을 형성한다.

<BAC 상호인증>

BAC를 지원하는 판독시스템이 광학적으로 읽은 MRZ로부터 생성한 BAC 인증키를 이용하고 TOE는 DG1의 MRZ 정보로부터 BAC 인증키를 생성하거나 저장된 BAC 인증키를 이용하여 각각 생성한 난수값을 암호화하여 상호 교환한다. BAC를

지원하는 판독시스템과 TOE는 상호 교환한 난수값을 확인함으로써 상호인증을 수행한다. BAC 상호인증이 실패한 경우에는 세션을 종료한다.

<EAC-CA>

EAC-CA는 EAC 세션키 분배와 칩 인증을 제공하기 위해 Ephemeral-static DH 키 분배 프로토콜을 구현한 것이다. TOE는 판독시스템이 자신을 인증할 수 있도록 EAC 칩 인증 공개키를 전송하고 판독시스템으로부터 받은 임시 공개키를 이용하여 키 분배 프로토콜을 수행한다. EAC-CA 과정이 성공하면 TOE는 EAC 세션 키를 이용하여 EAC 안전한 통신채널을 형성한다. EAC-CA가 실패한 경우도 BAC 안전한 통신채널은 유지되며 판독시스템은 TOE가 불법 복제되었음을 확인할 수 있다.

<EAC-TA>

EAC-TA는 TOE가 EAC를 지원하는 판독시스템을 인증하기 위해 전자서명 기반 Challenge-Response 인증 프로토콜을 구현한 것이다. EAC-CA 과정에서 사용한 임시 공개키에 판독시스템이 전자서명한 값을 TOE가 IS 인증서를 이용하여 검증함으로써 판독시스템을 인증한다. TOE는 EAC를 지원하는 판독시스템으로부터 CVCA 링크인증서, DV 인증서, IS 인증서를 수신하면, 보호메모리영역에 있는 CVCA 전자서명검증키를 이용하여 CVCA 링크인증서를 검증하고, CVCA 링크인증서의 유효 기간을 확인하여 필요 시 TOE 내 CVCA 전자서명검증키 및 현재 날짜를 갱신한다. TOE는 IS 인증서를 검증하여 적합한 인증서임을 확인하면 EAC를 지원하는 판독시스템의 전자여권 신청인 인코딩된 전자여권 소지자 정보에 대한 읽기 접근을 허용하고 EAC 안전한 통신채널을 통해 전송한다.

<PA>

TOE는 BIS, EIS에게 SOD를 제공함으로써 판독시스템이 SOD 전자서명 검증을 통해 전자여권 사용자 데이터의 위변조를 탐지하도록 하여 PA 보안메커니즘을 지원한다.

<AA>

AA(Active Authentication)는 판독시스템이 TOE를 인증하기 위해 전자서명 기반 Challenge-Response 인증 프로토콜을 구현한 것이다. 판독시스템이 제공한 전송값에 TOE가 보호메모리 영역에 있는 AA 칩 인증 개인키로 전자서명을 생성하여 전송하면, 판독시스템은 BAC 안전한 통신채널 또는 EAC 안전한 통신채널을 통해 획득한 EF.DG15 AA 칩 인증 공개키로 검증함으로써 TOE를 인증한다. AA는 TOE의 불법복제여부를 검증하기 위한 수단을 제공하는 보안메커니즘이다.

· 사용자 데이터 보호

TOE는 사용자 데이터 보호를 위해 접근통제와 안전한 통신채널을 제공한다.

<SCP02 안전한 통신 채널>

TOE는 SCP02 상호인증 과정을 성공적으로 수행한 발급기관과 안전한 통신을 수행하기 위해 SCP02 상호인증 과정에서 생성한 SCP02 세션 키를 이용하여 SCP02 안전한 통신채널을 수립한다. SCP02 안전한 통신 채널을 통해 데이터를 전송할 때 TDES 암호 알고리즘을 이용하여 데이터를 암호화 하여 비밀성을 제공하고 Retail MAC알고리즘을 이용한 MAC 검증을 통해 무결성을 제공한다.

<BAC 안전한 통신 채널>

TOE는 BAC 상호인증 과정을 통해 전자여권 신청인 기본정보에 대한 판독시스템의 읽기권한을 확인한 후 전자여권 신청인 기본정보를 안전하게 전송하기 위해 BAC 키분배를 통해 공유한 BAC 세션 키를 이용하여 BAC 안전한 통신 채널을 생성한다. BAC 안전한 통신채널을 통해 데이터를 전송할 때 TDES 암호 알고리즘으로 데이터를 암호화 하여 비밀성을 제공하고 Retail MAC 알고리즘을 이용한 MAC 검증을 통해 무결성을 제공한다.

<EAC 안전한 통신 채널>

TOE는 판독시스템과 안전한 통신을 수행하기 위해 EAC-CA과정의 EAC 키분배를 통해 공유한 EAC 세션 키를 이용하여 EAC 안전한 통신채널을 생성한다. EAC 안전한 통신채널을 통해 데이터를 전송할 때 TDES 암호 알고리즘으로 데이터를 암호화하여 비밀성을 제공하고, Retail MAC 알고리즘을 이용한 MAC 검증을 통해 무결성을 제공한다.

<운영체제 접근통제>

TOE는 SCP02 상호인증을 성공하여 관리권한을 획득한 발급기관만이 전자여권 발급단계 및 사용단계에서 개방형 운영체제에 실행파일 및 응용프로그램을 탑재, 설치, 삭제하는 응용프로그램 관리기능과 발급기관의 기본정보에 대한 쓰기기능을 수행하도록 접근통제 기능을 제공한다. 또한 TOE의 생명주기가 종료단계에서 발급기관 기본정보에 대한 읽기기능을 제외한 모든 오퍼레이션이 수행되지 않도록 접근통제 기능을 제공한다.

<전자여권 접근통제>

TOE는 SCP02 상호인증을 성공하여 발급권한을 획득한 발급기관만이 전자여권의 발급 단계에서 전자여권 사용자 데이터 및 TSF 데이터에 대한 쓰기기능을 수행하도록 접근통제 기능을 제공한다. 또한, 전자여권 사용 단계에서 보안메커니즘 수행을 통해 부여된 판독시스템의 접근권한에 기반하여 전자여권 사용자 데이터의 읽기권한에 대한 접근통제 기능을 제공한다.

· 보안관리

TOE는 발급단계에서 요구되는 전자여권 응용프로그램 및 운영체제의 사용자 및 사용자 데이터의 보안속성과 세션키, 인증키 및 GP 레지스트리와 같은 TSF 데이터를 관리하는 수단을 인가된 발급기관으로만 제한하고 이를 보안역할로 정의한다. 또한 전자여권의 CVCA 인증서 및 현재 날짜 갱신, 안전한 통신채널 식별 정보 초기화 등 일부 보안관리 기능에 대해 TSF가 자체적으로 수행한다.

· TSF 보호

TOE는 TSF보호를 위해 참조모니터, 영역분리, 잔여정보 삭제, 트랜잭션 처리 및 자체시험의 기능을 제공한다.

<참조모니터>

TOE는 신뢰되지 않은 주체에 의한 간섭과 침해로부터 TSF를 보호하기 위해 TOE 외부 인터페이스인 모든 APDU 명령어에 대해 접근통제 기능이 우회되지 않고 항상 호출될 것을 보장한다.

<영역분리>

TOE는 다른 응용프로그램 등 신뢰되지 않은 주체가 사용하는 영역과 전자여권 응용프로그램이 수행되는 영역을 분리하기 위해 자바카드 가상 머신 내에 자바카드 방화벽(Java Card Firewall)을 제공한다.

<잔여정보 삭제>

TOE는 BAC세션키, EAC 세션키, SCP02 세션키, 난수 등의 임시메모리 영역에 일시적으로 생성되는 정보뿐만 아니라 BAC 인증키 등 보호메모리 영역에 생성되는 정보에 대해서도 객체에 자원을 할당하거나 객체로부터 자원을 회수할 때 이전의 정보가 가용하지 않도록 잔여정보를 삭제하는 기능을 제공한다.

<트랜잭션 처리>

TOE는 동작도중에 전원공급 중단 및 강제적인 TSF 서비스의 종료가 발생된 경우 TSF의 장애를 검출하여 장애 이전의 상태로 TSF 서비스를 개시하도록 하기 위해 트랜잭션 기능을 제공한다.

<자체시험>

TOE는 전송되는 TSF 데이터의 변경 탐지 및 대응 기능을 수행하고, 저장된 TSF 데이터 및 실행코드의 무결성을 검증하기 위한 자체시험을 한다. 또한, 자체시험을 통해 실패를 탐지하거나 IC 칩에서 비정상 동작 상태를 탐지하여 알려주는 경우 TSF의 오동작이 발생하지 않도록 안전한 상태를 유지한다.

· **암호지원**

TOE는 해시연산을 제공하며, IC칩 및 암호연산 라이브러리를 이용하여 난수 생성, 키교환 연산 운영모드, 암복호화 연산 운영모드, MAC 및 전자서명 연산 운영모드를 제공한다.

TOE는 암호 연산 수행 시 발생하는 물리적 현상(전류, 전압, 전자기 변화 등)을 악용하여 암호 관련 정보를 알아내지 못하도록 보장하며, 암호키에 대한 무결성 검증의 수단을 제공한다.

6. 설명서

평가제품이 제공하는 설명서는 아래와 같다.

- XSmart e-Passport V1.1 설명서 V1.0

7. 제품시험

7.1 개발자 시험

- **시험방법**

개발자는 제품의 보안기능을 고려하여 시험항목을 도출하였다. 각 시험항목은 시험서에 서술되어 있다. 시험서에 서술된 각 시험항목은 아래의 세부 항목을 포함하고 있다:

- 시험번호/시험자 : 시험항목 식별자 및 시험에 참여한 개발자
- 시험목적 : 시험 대상 보안기능 및 보안모듈을 포함하여 시험의 목적을 서술
- 시험환경 : 시험을 수행하기 위한 세부 시험환경
- 세부 시험절차 : 보안기능을 시험하기 위한 세부 절차
- 예상결과 : 시험절차를 수행하였을 때 나타날 것으로 예상되는 시험결과
- 실제결과 : 시험절차를 실제로 수행하였을 때 나타나는 시험결과
- 예상결과와 실제결과의 비교 : 예상결과 및 실제결과를 비교한 결과

평가자는 시험서의 시험환경, 시험절차, 시험범위 분석, 상세설계 시험 등 시험의 타당성을 평가하였다. 평가자는 개발자의 시험 및 시험결과가 평가환경에 적합함을 검증하였다.

- **시험환경**

시험서에 서술된 시험환경은 시험을 위한 구성, 평가대상제품, 내부망 및 외부망 등 세부 환경을 포함하고 있다. 또한, 각 시험항목을 시험하기 위해 필요한 시험도구 등 세부적인 시험환경을 서술하고 있다.

- **시험범위 분석/상세설계 시험**

세부 평가결과는 ATE_COV 및 ATE_DPT 평가결과에 서술되어 있다.

- **시험결과**

시험서는 각 시험항목의 예상결과 및 실제결과를 서술하고 있다. 실제결과는 실제 제품의 동작화면 뿐만 아니라 감사기록을 통해서도 확인할 수 있다.

7.2 평가자 시험

평가자는 개발자 시험과 동일한 평가환경 및 평가도구를 사용하여 평가제품을 설치하고 개발자가 제공한 시험항목 전체를 시험하였다. 평가자는 모든 시험항목에서 실제결과가 예상결과와 일치함을 확인하였다.

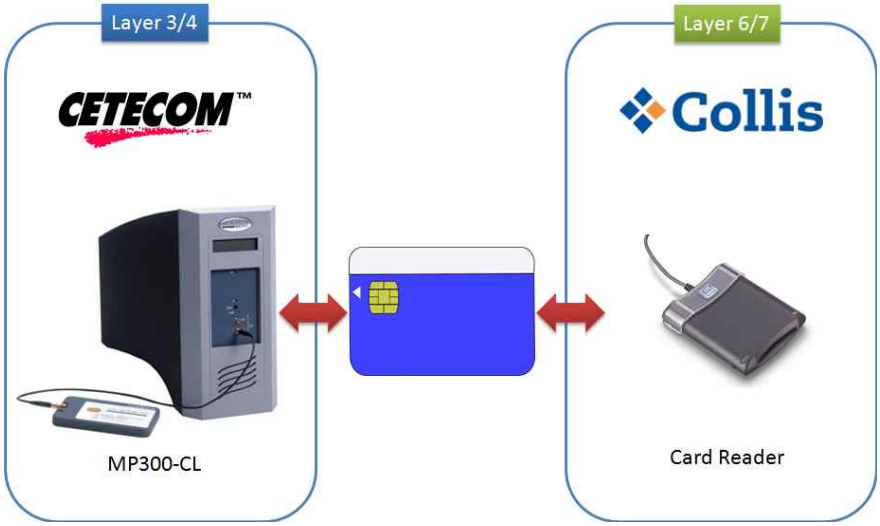
또한, 평가자는 개발자 시험에 기초하여 별도의 평가자 시험항목을 고안하여 시험한 결과, 실제결과가 예상결과와 일치함을 확인할 수 있었다.

평가자는 취약성 시험을 수행한 결과, 평가환경에서 어떠한 취약성도 악용 가능하지 않다는 점을 확인하였다.

평가자의 시험결과는 평가제품이 설계문서에 서술된 대로 정상적으로 동작됨을 보증하였다.

8. 평가환경

평가자는 시험을 위해서 보안목표명세서에서 명시된 환경구성과 일관성 있게 시험환경을 [그림 4]와 같이 구성하였다.



[그림 4] 평가자 시험환경

9. 평가결과

평가는 최신 공통평가기준, 공통평가방법론을 적용하였다. 평가는 평가제품이 공통평가기준 2부, EAL4+ 평가보증등급의 요구사항 3부에 적합하다고 평가하였다. 자세한 평가결과는 평가보고서에 서술되어 있다.

- **보안목표명세서**

보안목표명세서 소개는 보안목표명세서 및 TOE를 정확하게 식별하고, TOE를 세 단계의 추상화 수준(TOE 참조, TOE 개요, TOE 설명)에서 정확하게 서술하며, 이 세 단계의 서술이 서로 일관성이 있으므로 ASE_INT.1에 대하여 통과 판정을 부여한다.

준수 선언은 보안목표명세서가 준수하는 공통평가기준에 대한 준수 선언을 정당하게 서술하고 있으므로 ASE_CCL.1에 대하여 통과 판정을 부여한다.

보안문제정의는 TOE 및 TOE의 운영 환경에서 다루어져야 하는 보안 문제를 명확히 정의하고 있으므로 ASE_SPD.1에 대하여 통과 판정을 부여한다.

보안목적은 적절하고 완전하게 보안 문제 정의를 다루고 있으며, TOE 및 TOE 운영 환경에서의 보안 문제를 명확히 분류하여 보안문제를 정의하고 있으므로 ASE_OBJ.2에 대하여 통과 판정을 부여한다.

확장 컴포넌트가 존재하지 않으며 ASE_ECD.1-1 ~ ASE_ECD.1-13 작업단위 평가활동이 적용 가능하지 않으므로 ASE_ECD.1에 대하여 통과 판정을 부여한다.

보안요구사항이 명확하고 모호하지 않으며 잘 정의되어 있으므로 ASE_REQ.2에 대

하여 통과 판정을 부여한다.

TOE 요약명세에서 모든 SFR을 다루고 있으며, TOE 요약명세가 TOE의 다른 서술적인 설명과 일관성이 있으므로 ASE_TSS.1에 대하여 통과 판정을 부여한다.

따라서, 보안목표명세서는 타당하고 내부적으로 일관성 있으며, TOE 평가를 위한 기초 자료로 사용하기에 적합하다.

- **개발**

보안구조설명서는 TSF가 침해되거나 우회될 수 없도록 구성되었고, 보안 영역을 제공하는 TSF가 이러한 영역들을 서로 분리함을 적절히 서술하고 있으므로 ADV_ARC.1 컴포넌트에 대해 통과 판정을 부여한다.

기능명세서는 TSFI(SFR-enforcing, SFR-supporting, SFR-non interfering)에 대해 목적, 사용방법, 입력 매개변수, 오퍼레이션, 오류 메시지를 동등한 상세수준으로 명세하여서 TSFI를 정확하고 완전하게 준정형화된 방식으로 서술하고 있으므로 ADV_FSP.5 컴포넌트에 대해 통과 판정을 부여한다.

구현의 표현은 다른 평가자 분석활동에 이용하기에 적합하며, TSF의 상세한 내부 동작을 파악하기에 충분하므로 ADV_IMP.2 컴포넌트에 대해 통과 판정을 부여한다.

TSF 내부는 내부가 잘 구조화된 TSF는 구현이 용이하고, 취약성을 발생시킬 수 있는 결함을 포함할 가능성이 낮으며, 결함의 발생 없이 유지하기 용이하므로 ADV_INT.2 컴포넌트에 대해 통과 판정을 부여한다.

TOE 설계서는 TSF 설명을 위한 배경 및 전체 TSF 설명을 제공하며, TSF 경계를 결정하기에 충분하게 TOE에 대한 설명을 서브시스템의 관점으로 제공하고, TSF 내부에 대한 설명을 모듈의 관점으로 제공한다. 또한 SFR이 완전하고 정확하게 구현되었음을 결정하도록 SFR-수행 모듈에 대한 상세한 설명과 SFR-지원 및 SFR-비-간섭 모듈에 대한 충분한 정보를 제공한다. 이로써 TOE 설계는 구현의 표현에 대한 설명을 제공하고 있으므로, ADV_TDS.4컴포넌트에 대해 통과 판정을 부여한다.

따라서 설계 문서에 포함된 보안구조설명서(TSF 보안 수행이 손상되거나 우회되지 않는 방법을 설명하는 TSF의 구조 속성), 기능명세서(TSF 인터페이스 설명), 설계서 및 구현의 표현(선언된 SFR과 관련된 기능을 수행하기 위하여 TSF가 어떻게 동작하는지 구조 설명), 구현의 표현(소스코드 수준의 설명)는 TSF가 SFR을 만족하는 방법을 이해하고, 이러한 SFR 구현이 침해 또는 우회되지 않는 방법을 이해하기에 적절하다.

- **설명서**

발급설명서 및 사용설명서는 각 사용자 역할별로 TSF가 제공하는 보안 기능성 및 인터페이스에 대하여 설명하고, TOE를 안전하게 사용하기 위한 지침 및 가이드라인을 제공하며, 모든 운영모드에 대한 안전한 절차를 다루고, TOE의 불안전한 상태 탐지 및 방지를 용이하게 하며, 오해의 소지가 있거나 비합리성이 존재하지 않으므로 AGD_OPE.1 컴포넌트에 대해 통과 판정을 부여한다.

TOE는 전자여권 애플릿 설치과정이 개발단계에 포함되어 있어, 별도의 설치과정이 필요하지 않으므로 AGD_OPE.1 컴포넌트는 적용되지 않는다. 따라서 AGD_PRE.1 컴포넌트에 대해 통과 판정을 부여한다.

따라서, 발급설명서 및 사용설명서는 사용자가 TOE를 안전한 방식으로 다룰 수 있는 방법을 적절하게 서술하고 있다.

- **생명주기 지원**

형상관리문서는 개발자가 TOE와 TOE 관련 형상항목을 명확히 식별하며, 이들 형상항목을 변경하는 능력이 자동화된 도구에 의해 적절하게 통제되고, 그 결과로 형상관리 시스템에서 사람의 실수 또는 태만에 의해 발생하는 오류가 감소함을 입증하므로 ALC_CMC.4에 대해 통과 판정을 부여한다.

형상관리문서는 형상목록에 TOE, TOE 구성 요소, TOE 구현의 표현, 보안결함, 평가제출물, 개발도구를 포함하고 있음을 입증하므로 ALC_CMS.5에 대해 통과 판정을 부여한다.

배포절차서는 TOE를 사용자에게 배포할 때 TOE 보안 유지를 위한 모든 절차를 서술하고 있으므로 ADO_DEL.1 컴포넌트에 대해 통과 판정을 부여한다.

개발보안문서는 TOE의 안전한 운영이 손상되지 않도록 보장하기 위하여 TOE 설계 및 구현에 대한 비밀성 및 무결성을 제공하기 위해 개발자가 개발 환경에 적용하는 보안 통제가 적절함을 보장하므로 ALC_DVS.1 컴포넌트에 대해 통과 판정을 부여한다.

개발자가 생명주기문서에 문서화된 TOE 생명주기 모델을 사용하고 있음을 확인하였으므로 ALC_LCD.1 컴포넌트에 대해 통과 판정을 부여한다.

개발자가 일관성 있고 예측할 수 있는 결과를 낼 수 있는 적용된 구현 표준을 따르는 개발 도구를 사용했음을 확인하였으므로 ALC_TAT.2 컴포넌트에 대해 통과 판정을 부여한다.

따라서, 생명주기 관련 문서는 개발자가 TOE를 구현하고 유지 보수하는 동안 사

용한 보안 절차가 적절한지 결정하기 위한 절차로써 개발자가 사용한 생명주기 모델, 형상관리, TOE 개발 전반에 걸쳐서 사용된 보안 대책, TOE 생명주기 전반에 걸쳐서 개발자가 사용한 도구 및 배포 활동을 적절하게 서술하고 있다.

- **시험**

시험서는 개발자가 TSFI를 시험하였고, 개발자가 시험서의 시험항목과 기능명세서의 TSFI 사이의 일치성을 보여줄 수 있는 증거를 제시하였음을 입증하므로 ATE_COV.2 컴포넌트에 대해 통과 판정을 부여한다.

시험서는 TSF 서브시스템 및 SFR-수행 모듈이 TOE 설계 및 보안구조 설명에서 서술된 것과 같이 동작하고 상호작용함을 입증하므로 ATE_DPT.3 컴포넌트에 대해 통과 판정을 부여한다.

시험서는 개발자가 시험서에 서술된 시험항목을 정확히 수행하고 문서화함을 입증하므로 ATE_FUN.1 컴포넌트에 대해 통과 판정을 부여한다.

평가자는 TSF 일부에 대한 독립적인 시험을 수행하여 TOE가 명세된 대로 동작함을 확인하였고, 개발자 시험에 대한 전수시험을 통하여 개발자가 수행한 시험에 대한 신뢰를 얻었으므로 ATE_IND.2 컴포넌트에 대해 통과 판정을 부여한다.

따라서, 시험서를 통해 TSF가 설계문서에 명세된 대로 동작하며 보안목표명세서에 명세된 TOE 보안기능요구사항에 부합하여 동작함을 확인하였다.

- **취약성 평가**

평가자는 중간의 공격성공 가능성을 지닌 공격자에 의한 잠재적인 취약성이 TOE 운영 환경에서 악용될 수 없음을 확인하였으므로 AVA_VAN.4 컴포넌트에 대해 통과 판정을 부여한다.

따라서, 개발 평가 및 예상되는 TOE 운영 시 또는 기타 방법에 의해 식별된 잠재적인 취약성이 공격자가 SFR을 위반할 수 없음을 확인하였다.

10. 권고 사항

평가 받은 TOE 운영환경에서만 TOE의 안전성을 보장할 수 있으므로 다음의 가정사항을 반드시 준수하여 TOE를 운영하여야 한다.

① TOE에서 기본으로 제공하는 전자여권 응용프로그램 이외에 별도의 응용프로그램을 탑재할 경우, 해당 어플리케이션이 스마트카드 운영체제 및 전자여권 응용프로그램에 보안 위협이 되지 않는지 검토하여야 한다.

11. 약어 및 용어 정의

아래의 약어 및 용어가 본 보고서에서 사용되었다.

CC	공통평가기준(Common Criteria)
EAL	평가보증등급(Evaluation Assurance Level)
PP	보호프로파일(Protection Profile)
SOF	기능강도(Strength of Function)
ST	보안목표명세서(Security Target)
TOE	평가대상(Target of Evaluation)
TSF	TOE 보안기능(TOE Security Functions)

발급기관 (Personalization Agent)	전자여권 신원정보 등을 접수 및 교부기관으로부터 받아 이에 대해 전자서명하여 SOD를 생성하고 이들을 전자여권 IC 칩에 기록한 후 전자여권 TSF 데이터를 생성하여 전자여권 IC 칩의 보호메모리영역에 저장하는 기관이며 PA-PKI 및/또는 EAC-PKI 를 운영하는 기관
여권 전자서명	전자적 방법으로 처리된 여권의 발급 및 기재 수록사항의 확인등을 위해 발급기관이 여권전자서명체계에서 발급한 전자서명 생성키로 전자여권에 서명한 고유 정보
전자여권 (ePassport)	국제민간항공기구(ICAO)와 국제표준화기구(ISO)에서 규정하는 국제표준에 따라 여권 신청인의 신원정보 및 기타 정보가 저장된 비접촉식 IC 칩(Contactless IC Chip)을 내장한 여권
전자여권 사용자 데이터	전자여권 신원정보, 전자여권 인증정보를 포함
전자여권 신원정보	전자여권 신청인 기본정보와 전자여권 신청인 바이오정보를 포함
전자여권 신청인 기본정보	전자여권 신원정보면에 인쇄되어 육안으로 식별할 수 있는 정보와 기타 신원정보가 LDS 구조로 전자여권 IC 칩에 저장된 정보
전자여권 신청인 바이오정보 (Sensitive Data)	전자여권 신청인의 지문 및/또는 홍채 정보가 LDS 구조로 전자여권 IC 칩에 저장된 정보
전자여권 응용데이터	전자여권 사용자 데이터, 전자여권 TSF 데이터를 포함
전자여권 응용프로그램 (MRTD Application)	전자여권 규격의 LDS에 따라 프로그래밍되고, BAC, PA, EAC 등 보안 메커니즘을 제공하는 전자여권 IC 칩 탑재용 프로그램

판독 (Inspection)	출입국 관리기관이 전자여권 소지자가 제시한 전자여권 IC 칩을 조사하여 전자여권 IC 칩의 진위 검증을 통해 전자여권 소지자의 신분을 확인하는 절차
판독시스템 (IS : Inspection System)	전자여권 판독을 지원하기 위해 광학적 MRZ 가독 기능 및 보안메커니즘(PA, BAC, EAC, AA 등)을 구현한 정보시스템으로 전자여권 IC 칩과의 RF 통신을 하는 단말기와 이 단말기를 통해 전자여권 IC 칩으로 명령어를 전송하고 이에 대한 응답을 처리하는 시스템으로 구성
AA (Active Authentication)	전자여권 IC 칩이 판독시스템으로부터 전송된 난수에 서명함으로써 판독시스템에게 자신의 진위성을 입증하고, 판독시스템은 서명값을 검증함으로써 전자여권 IC 칩의 진위성을 검증하는 보안 메커니즘
BAC (Basic Access Control)	전자여권 IC 칩과 판독시스템의 상호인증을 위한 대칭키 기반 실체인증 프로토콜과 전자여권 IC 칩과 판독시스템의 안전한 통신채널 형성에 필요한 세션키 생성을 위한 대칭키 기반 키분배 프로토콜을 구현한 보안메커니즘
BAC 상호인증	ISO 9798-2 대칭키 기반 실체인증 프로토콜에 따라 전자여권 IC 칩과 판독시스템을 상호인증하는 것
BAC 판독시스템 (BIS : BAC Inspection System)	BAC, PA, AA 보안메커니즘을 구현한 판독시스템
EAC (Extended Access Control)	전자여권 IC 칩에 저장된 전자여권 신청인 바이오정보에 대한 접근통제를 위해 EAC를 지원하는 판독시스템(EIS)만이 전자여권 신청인 바이오정보를 읽을 수 있도록 칩인증을 위한 EAC-CA과정과 판독시스템 인증을 위한 EAC-TA 과정으로 구성된 보안메커니즘
EAC 판독시스템 (EIS : EAC Inspection System)	BAC, PA 및 EAC 보안메커니즘을 구현하고 AA를 옵션으로 구현한 판독시스템
EAC-CA (EAC-Chip Authentication)	전자여권 IC 칩의 EAC 칩인증 공개키 및 개인키와 EIS의 임시 공개키 및 개인키에 대한 키확인을 통해 EAC를 지원하는 판독시스템이 전자여권 IC 칩을 인증할 수 있도록 Ephemeral-Static DH 키분배 프로토콜(PKCS#3, ANSI X.42 등)을 구현한 보안메커니즘
EAC-TA (EAC-Terminal Authentication)	EIS가 EAC-CA 과정에서 사용한 임시 공개키에 자신의 전자서명생성키로 전자서명하여 전송한 값을 전자여권 IC 칩이 IS 인증서를 이용하여 전자서명을 검증함으로써 전자여권 IC 칩이 EIS를 인증하는 전자서명 기반 Challenge-Response 인증 프로토콜을 구현한 보안메커니즘
LDS (Logical Data Structure)	전자여권 사용자 데이터를 전자여권 IC 칩에 저장하기 위해서 전자여권 규격에서 정의한 논리적 자료 구조
PA (Passive Authentication)	DS 인증서를 가진 판독시스템이 SOD에 서명된 전자서명을 검증하고 전자여권 접근통제 정책의 읽기권한에 따라

해당 전자여권 사용자 데이터의 해시값을 검증하여 전자여권에 기록된 신원정보가 위변조되지 않았음을 증명하는 보안메커니즘

12. 참고문헌

인증기관은 아래의 문서를 사용하여 본 인증결과보고서를 작성하였다.

[1] 정보보호시스템 공통평가기준 (2009. 9. 1)

[2] 정보보호시스템 공통평가방법론 V3.1

[3] 정보보호시스템 평가·인증 지침 (2009. 9. 1)

[4] 정보보호시스템 평가·인증업무 수행 규정 (2010. 1. 1)

[5] XSmart e-Passport V1.1 보안목표명세서 V1.4 (2010. 6. 9)

[6] XSmart e-Passport V1.1 평가결과보고서, 발행버전 1.0 (2010. 6. 25)