교육부

KERIS
한국교육학술정보원

교육행정전자서명
인증서처리프로그램 사양서

2019. 08

교육부
행정전자서명인증센터
Education Public Key Infrastructure Center

1. 개 요

본 문서는 교육부 행정전자서명인증센터 인증서비스 활용에 필요한 인증서처리프로그램(구 표준보안API)의 소개 및 주요 기능들을 정리하여 제공하는데 목적이 있다.

2. 인증서처리프로그램의 소개

인증서처리프로그램은 교육부 GPKI 인증서와의 연동을 통하여 보안서비스를 제공하는 응용프로그램을 만들기 위한 도구이다. 암호에 대한 배경 지식이 많지 않은 개발자도 필요한 보안사항에 따라 인증서처리프로그램 모듈을 사용하면 그에 대한 보안서비스를 제공하는 프로그램을 손쉽게 개발할 수 있다.

2.1. 인증서처리프로그램 사용 및 관리

인증서처리프로그램의 사용・관리는 아래내용을 따르도록 한다.

- 인증서처리프로그램을 제공 받은 기관은 인증센터에 사용 요청한 용도 이외에는 사용할 수 없으며, 타 용도로 사용하고자 할 때에는 인증센터와 협의하여야 한다.
- 사용기관은 인증서처리프로그램 전담 관리자를 지정하여 안전하게 관리하여야 하며, 인증서처리프로그램의 파손 등 보안사고 발생 또는 시스템 변경 등으로 인증서처리프로그램 미사용 시에는 관련 사실을 인증센터에 통보하여야 한다.
- 사용기관은 인증서처리프로그램 적용완료 또는 적용변경의 경우, <별지 서식>에 의거 “교육행정전자서명 인증서처리프로그램 적용결과표”를 작성하여 인증센터에 즉시 통보하여야 한다.

2.2. 인증서처리프로그램의 기능

2.2.1. 인증서 검증

모든 PKI동작에서는 자신 또는 상대방 인증서의 상태확인을 하는 동작이 필요하다. 이를 인증서 검증이라고 한다. 인증서 검증의 수행은 우선 검증하고자 하는 인증서의 경로검증과 유효기간, 기본정책을 검증한 후 인증서 폐지 유무를 판단하는 절차를 갖는다. 인증서 검증을 위해서는 인증서와 인증서 상태정보가 있어야한다.

- 파일에서 검증하고자 하는 인증서를 읽기 : 인증서 파일에서 인증서를 메모리로 읽어 들인다.
- 해당하는 인증서의 경로검증을 위한 상위 인증서 집합체를 생성 : 해당 디렉토리에서 인증경로상에 있는 인증서들을 가져와 구조체에 담는다.
- 인증서 유효성 검증 : 인증서 집합체에 있는 인증서에서 유효기간 정보를 읽어

드려 유효기간을 확인하고, 인증서 정책정보와 환경변수의 정책 정보값을 비교하여 유효한 정책정보를 가지고 있는지 확인한다.

- 키 쌍 검증 : 비공개키와 인증서에 포함된 공개키의 쌍이 맞는지 확인한다.
- 인증서 상태 검증 : 인증서 검증 요청시 SCVP는 클라이언트를 대신하여 서버가 인증 경로의 설정과 인증 경로를 검증하며, 인증서 정보 대한 요청문(CVRequest)를 생성하여 SCVP 서버에게 보내고 응답문(CVResponse)을 받아 인증서 검증을 한다 . 또는 인증서의 AIA필드에 있는 OCSP서버주소를 이용하여 인증서 상태정보를 가져온다. 인증서 AIA필드가 비어있는 경우 디렉토리의 CRL(ARL)정보를 통하여 인증서 폐지정보를 가져온다.

2.2.2. 사용자 인증

시스템에 접근하는 사용자가 정당한 사용자인지를 전자서명에 기반하여 인증한다.

- 사용자 인증 : 전자서명에 기반하여 서버의 난수를 받아 사용자가 서명하여 사용자를 인증한다.

2.2.3. 전자서명

서명자가 메시지에 대해 전자서명을 했을 때 그 서명이 다른 사람에 의해 위조되지 않았고, 서명된 후 그 내용이 변조되지 않았다는 것을 누구나 검증할 수 있다는 것을 말한다. 서명자가 자신의 비밀키를 사용하여 전자서명을 생성하여 수신자에게 보내고, 수신자는 서명자의 공개키를 사용하여 전자서명을 검증하는 과정이다.

- 비밀키 읽기 : 패스워드를 입력하여 비밀키를 얻는다.
- 전자서명 생성 : 주어진 메시지에 대하여 전자서명을 하여 PKCS#7 Signed Data 형태의 메시지를 만든다. 전자서명된 메시지에는 사용자의 인증서가 포함된다.
- 전자서명 검증 : 전자서명된 메시지에 대한 서명 검증을 수행한다. 전자서명된 메시지에는 사용자의 인증서가 포함되어 있으므로, 인증서 검증과정도 포함되어 있다.

2.2.4. 암호화

송신자는 수신자의 암호화용 공개키로 암호화하여 수신자에게 보내면 수신자는 자신의 암호화용 비밀키로 복호화할 수 있다. 이 과정에서 송신자는 디렉토리 시스템에 접근하여 수신자의 암호화용 공개키를 받아서 사용하는 부분이 포함된다.

- 암호화 : 세션키를 생성하여 메시지를 암호화하고, 세션키를 수신자의 암호화용 공개키로 암호화하여 보낸다.
- 복호화 : 수신자는 암호화된 세션키를 자신의 암호화용 비밀키로 복호화하여 암호화된 메시지를 복호화한다.

2.3. 인증서처리프로그램 지원환경

구성요소	개발환경	운영환경	비고
인증서처리 프로그램 서버	JAVA	UNIX(SUN, HP, AIX), LINUX	Java, JSP 기반 응용에 적용
	JAVA	WINDOWS	Java, JSP 기반 응용에 적용
	COM	WINDOWS	ASP, .NET 기반 응용에 적용
인증서처리 프로그램 클라이언트	WEB	WINDOWS	IE, Edge, Chrome, FireFox, Opera
	WEB	Mac OS X 10.8 ~ 10.11	Safari
	WEB	Linux CentOS 6.x	FireFox

2.4. 지원 알고리즘

기술표준에 명시된 전자서명, 암호 알고리즘, 해쉬알고리즘 및 MAC 알고리즘 등 행정전자서명인증서 활용에 필요한 기본 알고리즘을 지원한다.

3. 준용 표준규격

행정전자서명인증체계의 상호 운용성을 보장할 수 있도록 인증서처리프로그램이 준용해야 하는 알고리즘 표준규격과 데이터 형식 및 프로토콜 표준규격은 다음과 같다.

알고리즘 표준규격	암호화	• 공공기관 암호화용 알고리즘 • SEED : TTAS.KO-12.0004 : 128비트 블록암호알고리즘(SEED) • AES : FIPS 197 ADVANCED ENCRYPTION STANDARD (AES) • 3DES : FIPS PUB 46-3 DATA ENCRYPTION STANDARD • ARIA : KS X 1213, 128비트 블록 암호 알고리즘 ARIA • KCAC.TS.ENC : 암호 알고리즘 규격 (v1.21)
	전자 서명	• KCDSA : TTAS.KO-12.0001R1, 부가형 전자서명방식표준(KCDSA) • RSA : PKCS #1 v2.0 RSA Encryption Standard • KCAC.TS.DSIG : 전자서명 알고리즘 규격(v1.30)
	해쉬함수	• HAS-160 : TTAS.KO-12.0011/R2 해쉬함수표준-제2부 : 해쉬함수알고리즘표준(HAS-160) • SHA-1 : FIPS 180-1 Secure Hash Standard • SHA256 : FIPS 180-2 Secure Hash Standard • KCAC.TS.HASH : 해쉬 알고리즘 규격 (v1.20)
	난수 생성	• ANSI X9.62 RNG • FIPS 186-2 General Purpose RNG
	HMAC	• RFC2104 HMAC : Keyed-hashing for Message Authentication

데이터 형식 및 프로토콜 표준규격	객체 인증	• ISO/IEC IS 9798-3 Entity authentication - Part 3: Mechanisms using digital signature techniques
	ASN & DER Encoding	• ITU-T X.680 Information Technology Abstract Syntax Notation One (ASN.1) : Specification of basic notation • ITU-T X.690 Information Technology ASN.1 Encoding Rules Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules(DER)
	인증서/인증서폐지목록 형식	• RFC3280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile • ITU-T X.509 Information Technology Open Systems Interconnection The Directory : Authentication Framework (ISO/IEC 9594-8) • KCAC.TS.CERTPROF : 전자서명인증서 프로파일 규격 (v1.70) • KCAC.TS.CRLPROF : 전자서명인증서 효력정지 및 폐지목록 프로파일 규격 (v.1.50)
	실시간 인증서 상태확인	• RFC6960 Internet X.509 Internet Public Key InfrastructureOnlineCertificateStatusProtocol-OCSP • KCAC.TS.OCSP (실시간 인증서 상태확인 기술규격 v1.21)
	서버기반 인증서 검증	• RFC5055 Server-Based Certificate Validation Protocol-SCVP
	인증서 관리	• RFC6712Internet X.509 Public Key Infrastructure - HTTP Transfer for the Certificate Management Protocol (CMP)
	인증서 발급 신청 형식	• RFC4211 Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF) • KCAC.TS.CRMF : 인증서 요청형식 프로토콜 규격 (v1.21)
	CMS (Cryptographic Message Syntax)	• PKCS #7 v1.5 Cryptographic Message Syntax Standard
	Base64 Encoding	• RFC2045 Multipurpose Internet Mail Extensions(MIME) Part One : Format of Internet Message Bodies
	키 저장	• Private Key Information Syntax : PKCS #8 v1.2 Private-key Information Syntax Standard • Password-based Encryption : PKCS #5 v2.0 Password-based Encryption Standard • PKCS#11 v2.2 Cryptographic Token Interface Standard
	Directory System	• LDAP v3 Lightweight Directory Access Protocol (v3): Technical Specification • KCAC.TS.LDAP : 전자서명인증체계 디렉토리 프로토콜 규격 [v1.11]
	본인 확인	• KCAC.SIVID (식별번호를 이용한 본인확인 기술 규격 v1.21)
보안토큰 인증규격	저장 및 이용 규격	• KCAC.TS.HSMU : 보안토큰 기반 인증서 이용기술 규격[v2.4] • KCAC.TS.HSMS : 보안토큰 기반 인증서 저장형식 기술규격[v1.13]

<별지 서식> 교육행정전자서명 인증서처리프로그램 적용결과표

교육행정전자서명 인증서처리프로그램 적용결과표

○ 기 관 명 :
○ 업무명(시스템명) :
○ 적용분야 :

□ 개 요

○ 적용기간 : ’19. . . ~ . . (서비스개시일 : . .)

○ 적용응용시스템명 :

○ 적용서버 :

○ 인증서처리프로그램 버전 :

□ 적용 결과

○ 사용자 로그인 분야

구 성 도	적 용 함 수
	· 전자서명 – · 서명검증 – · 인증서검증 – · 본인확인 –

<세부설명>

-

-

○ 데이터 송·수신 분야

구 성 도	적 용 함 수
	· 전자서명 – · 서명검증 – · 인증서검증 – · 본인확인 –

<세부설명>

-

-

※ 적용코드 : <별첨>

○ 서버(컴퓨터)용 인증서 정보

서버명	서버 IP	인증서 DN	비고

□ 기타 의견 (적용시 불편사항 및 개선의견 등을 자유롭게 기재하여 주십시오)

○

○

○