전자서명 인증서 효력정지 및 폐지목록 프로파일 규격

Accredited Digital Signature Certificate Revocation List Profile

v1.50

2009년 9월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

전자서명 인증서 효력정지 및 폐지목록 프로파일 규격

Accredited Digital Signature Certificate Revocation List Profile

1. 개요

본 규격에서는 전자서명법에 따라 구축된 공인전자서명인증체계의 공인인증기관이 유·무선 공인인증서비스를 제공하는데 있어 필수적으로 요구되는 전자서명 공인인증서(이하 인증서) 효력정지 및 폐지목록 프로파일을 규정한다.

2. 규격의 구성 및 범위

본 규격은 [RFC3280]을 준수하여 전자서명인증체계에서 사용되는 인증서 효력정지 및 폐지 목록 프로파일 규격을 정의하고 있다.

첫 번째로 본문에서는 인증서 효력정지 및 폐지 목록 내 기본필드와 확장필드의 사용 목적 및 구조체 등을 정의하고 있으며, 두 번째로 부록에서는 최상위인증기관과 공인인증기관 및 가입자 소프트웨어가 인증서 효력정지 및 폐지 목록을 생성 및 처리하는데 필요한 요구사항들을 명시하고 있다.

3. 관련 표준 및 규격

3.1 국외 표준 및 규격

[X509]	ITU-T Recommendation X.509 (2000), *Information technology - Open Systems Interconnection - The Directory : public-key and attribute certificate frameworks*
[RFC2119]	IETF RFC 2119 (1997), *Key Words for use in RFCs to Indicate Requirement Levels*
[RFC2459]	IETF RFC 2459 (1999), *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*
[RFC3280]	IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*
[WAPCert]	WAP-211-WAPCert-20010522-a(2001), *WAP*

3.2 국내 표준 및 규격

[KCAC.TS.DSIG] KISA, KCAC.TS.DSIG, v1.30, *전자서명 알고리즘 규격*, 2009
[KCAC.TS.SIVID] KISA, KCAC.TS.SIVID, v1.21, *식별번호를 이용한 본인확인 기술규격*, 2009
[KCAC.TS.DN] KISA, KCAC.DN, v1.21, *전자서명인증체계 DN 규격*, 2009
[KCAC.TS.CERTPROF] KISA, KCAC.TS.CERTPROF, v1.70, *전자서명 인증서 프로파일 규격,* 2009

3.3 기타

해당사항 없음

4. 정의

4.1 전자서명법 용어 정의

본 규격에서 사용된 다음의 용어들은 전자서명법 및 동법 시행령, 공인인증기관의 시설 및 장비 등에 관한 규정(미래창조과학부 고시)에 정의되어 있다.

가) 인증서
나) 공인전자서명인증체계(이하 “전자서명인증체계”)
다) 가입자
라) 가입자 소프트웨어
마) 공인인증서

4.2 용어의 정의

가) 부분 인증서 효력정지 및 폐지목록 : 공인인증기관이 일정 개수의 인증서마다 상이한 분배점(distributionPoint)을 통하여 인증서 효력정지 및 폐지목록을 관리할 때 이에 해당되는 인증서 효력정지 및 폐지목록

4.3 용어의 효력

본 규격에서 사용된 다음의 용어들은 전자서명인증체계 전자서명 인증서 효력정지 및 폐지목록 프로파일의 구현 정도를 의미하는 것으로 [RFC2119]를 준용하며 다음과 같은 의미를 지닌다.

가) 해야한다, 필수이다, 강제한다 (기호 : M)
반드시 준수해야 한다.
나) 권고한다 (기호 : R)
보안성 및 상호연동을 고려하여 준수할 것을 권장한다.
다) 할 수 있다, 쓸 수 있다 (기호 : O)
주어진 상황을 고려하여 필요한 경우에 한해 선택적으로 사용할 수 있다.
라) 권고하지 않는다 (기호 : NR)
보안성 및 상호연동을 고려하여 사용하지 말 것을 권장한다.
마) 금지한다, 허용하지 않는다 (기호 : X)
반드시 사용하지 않아야 한다.
바) 언급하지 않는다, 정의하지 않는다 (기호 : -)
준수 여부에 대해 기술하지 않는다.

5. 약어

본 규격에서는 다음의 약어들이 적용된다.

가) CA : Certification Authority, 공인인증기관
나) CRL : Certificate Revocation List, 공인인증서 효력정지 및 폐지목록
다) OID : Object Identifier, 객체 식별자
라) DN : Distinguished Name, 식별명칭
마) SHA : Secure Hash Algorithm

6. 전자서명 인증서 효력정지 및 폐지목록 프로파일

6.1 인증서 효력정지 및 폐지목록 기본필드

기본필드는 인증서 효력정지 및 폐지목록의 버전, 발급자, 발급일자 등의 기본

정보를 나타낸다. 아래 정의된 기본필드는 인증서 효력정지 및 폐지목록에 모두 포함되어야 하며, 가입자 소프트웨어는 이를 처리해야 한다.

6.1.1 버전(Version)

버전 필드는 인코딩되는 인증서 효력정지 및 폐지 목록의 버전을 나타낸다.

인증서 효력정지 및 폐지 목록은 버전 2의 값을 가져야만 하며 이 값은 정수 1로 표현된다.

6.1.2 서명 알고리즘(Signature)

서명 알고리즘 필드는 공인인증기관이 인증서 효력정지 및 폐지목록을 생성할 때 사용하는 서명 알고리즘의 OID 값을 가진다. 사용하는 서명 알고리즘은 [KCAC.TS.DSIG]를 준수해야 한다.

6.1.3 발급자(Issuer)

발급자 필드는 인증서 효력정지 및 폐지 목록을 발급한 기관의 명칭을 DN 형식으로 표현하며 반드시 값을 가져야 한다. 여기서 DN 형식은 [KCAC.TS.DN]을 준수해야 한다.

6.1.4 발급일자(This Update)

발급일자 필드는 인증서 효력정지 및 폐지목록이 기관에서 발급된 시점을 나타낸다.

시각 정보는 GMT로 표현하며 2049년까지 UTCTime 형식을 사용하고 2050년부터는 GeneralizedTime 형식을 사용하여 인코딩하여야 한다.

6.1.5 다음 발급일자(Next Update)

다음 발급일자 필드는 기관이 다음 인증서 효력정지 및 폐지목록을 발급할 시점을 나타낸다.

다음에 발급되는 인증서 효력정지 및 폐지 목록은 이 필드에서 지정한 일자보다 이전에 발급되어야 한다.

시각 정보는 GMT로 표현하며 2049년까지 UTCTime 형식을 사용하고 2050년부터는 GeneralizedTime 형식을 사용하여 인코딩하여야 한다.

6.1.6 효력정지 및 폐지 목록(Revaked Certificates)

효력정지 및 폐지 목록 필드는 효력정지 및 폐지된 인증서의 목록을 인증서의 일련번호와 폐지된 날짜로 나타내며 CRL 엔트리 확장필드에 추가적인 정보가 제공될 수 있다.

단, 효력정지 및 폐지된 인증서가 없을 경우에는 효력정지 및 폐지 목록 필드는 인증서 효력정지 및 폐지목록에 나타나지 않는다.

6.2 인증서 효력정지 및 폐지 목록(CRL) 확장필드

6.2.1 발급자 공개키 식별자 (Authority Key Identifier)

발급자 공개키 식별자 확장필드는 인증서 효력정지 및 폐지목록 발급자의 인증서에 대한 공개키를 식별하기 위해 사용된다.

```
AuthorityKeyIdentifier ::= SEQUENCE {
  KeyIdentifier            [0]    KeyIdentifier         OPTIONAL,
  authorityCertIssuer      [1]    GeneralNames          OPTIONAL,
  authorityCertSerialNumber [2]   CertificateSerialNumber OPTIONAL  }
```

발급자의 공개키를 식별하기 위해서는 KeyIdentifier와 authorityCertIssuer, authorityCertSerialNumber를 모두 사용해야 한다. KeyIdentifier는 발급자 인증서의 소유자 공개키 정보 확장필드 내 subjectPublicKey 값을 SHA-1 해쉬 알고리즘으로 해쉬한 160비트 값을 OCTET STRING 형태로 저장한다.

발급자 공개키 식별자는 인증서 효력정지 및 폐지목록에 반드시 포함되어야 하며 가입자 소프트웨어는 이 확장필드를 처리할 수 있어야 한다.

이 확장필드는 non-critical로 설정되어야 한다.

6.2.2 발급자 대체 명칭 (Issuer Alternative Name)

발급자 대체 명칭 확장필드는 인증서 효력정지 및 폐지 목록을 발급하는 기관의 추가적인 명칭을 나타내며, 인증서비스 영역 내에서 사용되는 고유한 식별정보를 나타낼 수 있다.

이 확장필드는 발급기관의 실명을 나타낸다. 발급기관의 실명은 [KCAC.TS.SIVID]를 준수하여 한글로 realName 하위필드에 UTF8 형식으로 표현되어야 한다.

인증서 효력정지 및 폐지 목록은 발급자 식별정보를 포함한 본 확장필드를 포함할 수 있으며 가입자 소프트웨어는 이 확장필드를 처리할 수 있어야 한다.

이 확장필드는 non-critical로 설정되어야 한다.

6.2.3 인증서 효력정지 및 폐지 목록 번호 (CRL Number)

인증서 효력정지 및 폐지 목록 번호 확장필드는 인증서 효력정지 및 폐지 목록을 식별할 수 있는 일련번호를 나타낸다.

일련번호는 인증기관이 발급하는 각각의 인증서 효력정지 및 폐지목록에 대해 순차적으로 증가하는 양의 정수로 표현한다.

모든 인증서 효력정지 및 폐지 목록의 CRL Number는 20바이트를 넘을 수 없으며, 가입자 소프트웨어는 최대 20 바이트의 CRL Number를 처리할 수 있어야 한다.

이 확장필드는 non-critical로 설정되어야 한다.

6.2.4 인증서 효력정지 및 폐지목록 발급 분배점 (Issuing Distribution Point)

인증서 효력정지 및 폐지목록 발급 분배점 확장필드는 해당 인증서 효력정지 및 폐지 목록을 획득할 수 있는 위치 정보를 포함하며, 아래와 같이 정의된다.

```
issuingDistributionPoint ::= SEQUENCE {
        distributionPoint            [0] DistributionPointName    OPTIONAL,
        onlyContainsUserCerts        [1] BOOLEAN DEFAULT   FALSE,
        onlyContainsCACerts          [2] BOOLEAN DEFAULT   FALSE,
        onlySomeReasons              [3] ReasonFlags              OPTIONAL,
        IndirectCRL                  [4] BOOLEAN DEFAULT   FALSE }

DistributionPointName ::= CHOICE {
        fullName                     [0] GeneralNames,
        nameRelativeToCRLIssuer      [1] RelativeDistinguishedName }
```

부분 인증서 효력정지 및 폐지목록은 이 확장필드의 distributionPoint 하위필드를 반드시 포함해야 한다. 이 경우 DistributionPointName.fullName은 ldap 주소의 URI 형태를 사용해야 하며 [KCAC.TS.CERTPROF]에서 정의하는 인증서 효력정지 및 폐지 목록 분배점(CRL DP)과 동일해야 한다.

onlyContainsUserCerts, onlyContainsCACerts, onlySomeReasons 항목은 인증서 효력정지 및 폐지목록 발급 분배점 확장필드에는 포함되지 않는다.

인증서 효력정지 및 폐지목록의 범위가 CRL 발급자 이외의 발급기관들이 발급한 인증서들을 포함할 경우, CRL 발급자는 반드시 indirectCRL을 BOOLEAN 값 "TRUE"로 설정해야 한다. 각 엔트리를 담당하는 발급기관은 인증서 발급자 (Certificate Issuer) CRL 엔트리 확장필드에 의해 표시된다[6.3.4절 참조].

이 확장필드는 사용자 인증서 효력정지 및 폐지목록에 대해서 반드시 포함되어야 하며 모든 가입자 소프트웨어는 이 확장 필드를 처리할 수 있어야 한다.

이 확장필드는 critical로 설정되어야 한다.

6.3 CRL 엔트리 확장필드

6.3.1 효력정지 및 폐지 사유 (Reason Code)

효력정지 및 폐지 사유 확장필드는 인증서가 효력정지 및 폐지된 사유를 나타내고 다음과 같이 정의된다.

```
CRLReason ::= ENUMERATED {
        unspecified             (0),
        keyCompromise           (1),
        cACompromise            (2),
        affiliationChanged      (3),
        superseded              (4),
        cessationOfOperation    (5),
        certificateHold         (6),
        removeFromCRL           (7) }
```

각각의 폐지사유에 대한 설명은 다음과 같다.

폐지사유	내 용
unspecified	특별한 폐지 사유가 없는 경우에 사용하며 본 규격에서는 이 비트를 사용하지 않음
keyCompromise	인증서 소유자의 전자서명키가 손상된 경우에 사용함
cACompromise	인증서 발급자의 전자서명키가 손상된 경우에 사용함
affiliationChanged	소유자의 명칭 또는 기타 정보가 변경된 경우에 사용함
superseded	키 손상없이 인증서를 폐지하고자 하는 경우에 사용함
cessationOfOperation	더 이상 지정된 목적으로 인증서를 사용하지 않는 경우에 사용함
certificateHold	인증서 효력정지에 사용함
removeFromCRL	델타 인증서 효력정지 및 폐지 목록과 함께 사용되며 본 규격에서는 이 비트를 사용하지 않음

이 확장필드는 모든 엔트리에 포함되어야 하며 모든 가입자 소프트웨어는 이를 처리할 수 있어야 한다.

이 확장필드는 non-critical로 설정되어야 한다.

6.3.2 효력정지 시 수행 명령 (Hold Instruction Code)

효력정지 시 수행 명령 확장필드는 효력정지된 인증서를 처리하는 명령에 대하여 OID를 사용하여 나타낸다.

이 확장필드는 인증기관 및 가입자 소프트웨어에서 선택적으로 생성할 수 있다.

이 확장필드는 non-critical로 설정되어야 한다.

6.3.3 효력정지 및 폐지 일자 (Invalidity Date)

효력정지 및 폐지 일자 확장필드는 폐지 사유가 발생한 시점에 대한 정보를 나타내며 6.1.4의 인증서 효력정지 및 폐지 목록 발행 일자와는 구분된다.

시각 정보는 GMT로 표현하며 2049년까지 UTCTime 형식을 사용하고 2050년부터는 GeneralizedTime 형식을 사용한다.

이 확장필드는 인증기관 및 가입자 소프트웨어에서 선택적으로 생성, 처리할 수 있다.

이 확장필드는 non-critical로 설정되어야 한다.

6.3.4 인증서 발급자 (Certificate Issuer)

인증서 발급자 확장필드는 간접 CRL과 관련하여 CRL 내의 효력정지 및 폐지된 인증서의 발급 기관에 대한 명칭을 나타내며 해당 기관 인증서의 소유자를 [KCAC.TS.CERTPROF]에 따라 생성하여야 한다.

간접 CRL의 첫 번째 엔트리가 본 확장필드를 사용하지 않았다면 인증서의 발급자가 CRL의 발급자와 동일하다는 것을 의미하며, 첫 번째 엔트리 이후 후속 엔트리에서 본 확장필드가 없다면, 그 엔트리에 대한 인증서 발급자는 그 직전 엔트리의 인증서 발급자와 동일한 것으로 간주한다.

이 확장필드는 인증서 효력정지 및 폐지 목록 발행 기관이 선택적으로 생성할 수 있으며 모든 가입자 소프트웨어는 이 확장필드를 처리 할 수 있어야 한다.

이 확장필드는 critical로 설정되어야 한다.

부록 1. 전자서명 인증서 효력정지 및 폐지목록 프로파일 요약

가. 인증기관 전자서명 인증서 효력정지 및 폐지목록(ARL) 프로파일

1) 기본필드

#	필드명	ASN.1 type	Note	지원여부		비고
				생성	처리	
1	Version	INTEGER	0x1(버전 2)	m	m	
2	Signature	OID	자동할당	m	m	
3	Issuer		DN 규격 준수 C(Country)는 printableString, 그 이외의 속성값은 utf8String	m	m	[1]
	type	OID		m	m	
	value	printableString 또는 utf8String		m	m	
4	This Update	UTCTime	발급시점	m	m	
5	Next Update	UTCTime	최상위인증기관 정책에 따름	m	m	
6	Revoked Certificates					[2]
	userCertificate	INTEGER		m	m	
	revocationDate	UTCTime		m	m	
	crlEntryExtensions	Extensions				[3]
7	CRL Extensions	Extensions		m	m	[4]
[1]	C=KR,O=KISA,OU=Korea Certification Authority Central,CN=KISA RootCA 숫자 ※ (숫자) 1 : RSA, 2 : ECDSA					
[2]	효력정지 및 폐지된 인증서가 없을 경우는 Revoked Certificates 필드를 생성하지 않음					
[3]	아래 “3) ARL 엔트리 확장필드” 참조					
[4]	아래 “2) ARL 확장필드” 참조					

2) ARL 확장필드

#	필드명	ASN.1 type	Note	C	지원여부		비고
					생성	처리	
1	Authority Key Identifier			n	m	m	
	KeyIdentifier	OCTET STRING	최상위인증기관 인증서의 KeyID				
	authorityCertIssuer	GeneralNames					
	authorityCertSerialNumber	INTEGER					
2	Issuer Alternative Name	otherName	id-kisa-identifyData에 최상위인증기관 한글실명	n	o	m	
3	CRL Number	INTEGER		n	m	m	
4	Issuing Distribution Point			c	o	m	[1]
	DistributionPointName	IA5string			o	m	
	onlyContainsUserCerts	BOOLEAN			–	–	
	onlyContainsCACerts	BOOLEAN			–	–	
	onlySomeReasons	BIT STRING			–	–	
	indirectCRL	BOOLEAN			o	m	[2]
[1]	생성할 경우, CRLDP(Certificate Revocation List Distribution Point)와 동일 ※ [KCAC.TS.CERTPROF] 참조						
[2]	indirectCRL를 사용할 때는 반드시 “TRUE"로 설정						

3) ARL 엔트리 확장필드

#	필드명	ASN.1 type	Note	C	지원여부		비고
					생성	처리	
1	Reason Code	ENUMERATED		n	m	m	
2	Hold Instruction Code	OID		n	o	m	
3	Invalidity Date	UTCTime		n	o	m	
4	Certificate Issuer	GeneralNames		c	o	m	

나. 가입자 전자서명 인증서 효력정지 및 폐지목록(CRL) 프로파일

1) 기본필드

#	필드명	ASN.1 type	Note	지원여부		비고
				생성	처리	
1	Version	INTEGER	0x1(버전 2)	m	m	
2	Signature	OID	자동할당	m	m	
3	Issuer		[KCAC.TS.DN] 준수 C(Country)는 printableString, 그 이외의 속성값은 utf8String	m	m	
	type	OID		m	m	
	value	printableString 또는 utf8String		m	m	
4	This Update	UTCTime	발급시점	m	m	
5	Next Update	UTCTime	공인인증기관 정책에 따름	m	m	
6	Revoked Certificates					[1]
	userCertificate	INTEGER		m	m	
	revocationDate	UTCTime		m	m	
	crlEntryExtensions	Extensions				[2]
7	CRL Extensions	Extensions		m	m	[3]
[1]	효력정지 및 폐지된 인증서가 없을 경우는 Revoked Certificates 필드를 생성하지 않음					
[2]	아래 “3) CRL 엔트리 확장필드” 참조					
[3]	아래 “2) CRL 확장필드” 참조					

2) CRL 확장필드

#	필드명	ASN.1 type	Note	C	지원여부		비고
					생성	처리	
1	Authority Key Identifier			n	m	m	
	KeyIdentifier	OCTET STRING	인증기관 인증서의 KeyID				
	authorityCertIssuer	GeneralNames					
	authorityCertSerialNumber	INTEGER					
2	Issuer Alternative Name	otherName	id-kisa-identifyData에 인증기관 한글실명	n	o	m	
3	CRL Number	INTEGER		n	m	m	
4	Issuing Distribution Point			c	m	m	
	DistributionPointName	IA5string			m	m	[1]
	onlyContainsUserCerts	BOOLEAN			–	–	
	onlyContainsCACerts	BOOLEAN			–	–	
	onlySomeReasons	BIT STRING			–	–	
	IndirectCRL	BOOLEAN			o	m	[2]
[1]	CRLDP(Certificate Revocation List Distribution Point)와 동일 ※ [KCAC.TS.CERTPROF] 참조						
[2]	indirectCRL를 사용할 때는 반드시 “TRUE"로 설정						

3) CRL 엔트리 확장필드

#	필드명	ASN.1 type	Note	C	지원여부		비고
					생성	처리	
1	Reason Code	ENUMERATED		n	m	m	
2	Hold Instruction Code	OID		n	o	m	
3	Invalidity Date	UTCTime		n	o	m	
4	Certificate Issuer	GeneralNames		c	o	m	

부록 2. 규격 연혁

버전	제·개정일	제·개정내역
v1.00	2001년 6월	·TTAS.KO-12.0013으로 제정
v1.10	2004년 6월	· 무선 전자서명 인증서 효력정지 및 폐지목록 프로파일 규격 v1.21 흡수 통합 · 전체적인 문서 형식 및 구성을 전자서명인증관리체계 규격 문서양식에 맞게 개정 · 6. 전자서명 인증서 효력정지 및 폐지목록 프로파일을 RFC3280에 적합하게 내용 수정 · 부록 1. 기존의 부록을 RF3280에 적합하게 수정하고 ARL과 CRL을 구분하여 요약함
v1.30	2007년 4월	· 1. 개요에서 유·무선 통합에 따른 내용 변경
v1.40	2008년 10월	· 관련 국내 표준 및 규격 갱신 내용 반영 · 법률 공포번호가 해당 법률 개정시마다 변경되는 점을 고려하여 법령명으로 개정
v1.50	2009년 9월	· 참조 기술규격명 변경 사항 반영