인증센터

인증서 프로파일 규격

Version 1.2

Korea Information Certificate Authority Inc.

제.개정 이력

1.2	개정	2022/04
1.1	개정	2022/01
1.0	신규 제정	2018/09
개정번호	제.개정 페이지 및 내용	제.개정 일자

목 차

1. 목적 7

2. 규격의 구성 및 범위 7

3. 약어 7

4. 정의 7

4.1. 용어의 정의 8

4.2. 용어의 효력 8

5. 인증서 프로파일 8

5.1. 인증서 기본필드 8

5.1.1. 버전(VERSION) 9

5.1.2. 일련 번호(SERIAL NUMBER) 9

5.1.3. 서명 알고리즘(SIGNATURE) 9

5.1.4. 발급자(ISSUER) 9

5.1.5. 유효기간(VALIDITY) 9

5.1.6. 주체(SUBJECT) 9

5.1.7. 공개키(PUBLIC KEY) 9

5.2. 인증서 확장필드 10

5.2.1. 기관 키 식별자(AUTHORITY KEY IDENTIFIER) 10

5.2.2. 주체 키 식별자(SUBJECT KEY IDENTIFIER) 10

5.2.3. 키 사용(KEY USAGE) 10

5.2.4. 인증서 정책(CERTIFICATE POLICY) 10

5.2.5. 주체 대체 이름(SUBJECT ALTERNATIVE NAME) 10

5.2.6. 기본 제한(BASIC CONSTRAINTS) 10

5.2.7. 정책 제한 조건(POLICY CONSTRAINTS) 11

5.2.8. 확장된 키 사용(EXTENDED KEY USAGE) 11

5.2.9. CRL 배포 지점(CRL DISTRIBUTION POINTS) 11

5.2.10. 기관 정보 액세스(AUTHORITY INFORMATION ACCESS) 11

6. 인증서 효력정지 및 폐지목록 프로파일 11

6.1. 인증서 폐지목록 기본 필드 11

6.1.1. 버전(VERSION) 11

6.1.2. 서명 알고리즘(SIGNATURE) 11

6.1.3. 발급자(ISSUER) 12

6.1.4. 게시 날짜(THIS UPDATE) 12

6.1.5. 다음 업데이트(NEXT UPDATE) 12

6.1.6. 해지된 인증서(REVOKED CERTIFICATES) 12

6.2. 인증서 폐지목록 확장 필드 12

6.2.1. 기관 키 식별자(AUTHORITY KEY IDENTIFIER) 12

6.2.2. CRL 숫자(CRL NUMBER) 13

6.2.3. 배포 지점 발급 지점(ISSUING DISTRIBUTION POINT) 13

7. 부록 13

7.1. 최상위 인증기관 인증서 프로파일 13

7.2. 인증기관 인증서 프로파일 14

7.3. OCSP 인증서 프로파일 16

7.4. TSA 인증서 프로파일 19

7.5. 가입자 인증서 프로파일 21

7.6. 가입자 인증서 프로파일(싸인오케이서비스) 24

7.7. 인증기관 인증서 폐지목록(ARL) 프로파일 26

7.8. 가입자 인증서 폐지목록(CRL) 프로파일 27

인증센터 인증서 프로파일 규격

(Certification Center Certificate Profile)

1. 목적

본 문서는 한국정보인증주식회사(이하 "회사"라 한다)의 인증서비스를 제공하는데 있어 필수적으로 요구되는 인증서 프로파일을 규정한다.

2. 규격의 구성 및 범위

본 규격은 [RFC3280]을 준수하여 전자서명인증체계에서 사용되는 X.509 v3 인증서에 대한 프로파일 규격을 정의하고 있다.

3. 약어

본 규격에서는 다음의 약어가 이용된다.

1) DN : Distinguished Name, 식별명칭

2) ASN.1 : Abstract Syntax Notation One, 추상적 구문 표기

3) CPS : Certification Practice Statement, 인증업무준칙

4) CA : Certification Authority, 인증기관

5) CRL : Certificate Revocation List, 인증서 폐지목록

6) OID : Object Identifier, 객체 식별자

7) SHA : Secure Hash Algorithm

4. 정의

4.1. 용어의 정의

해당사항 없음

4.2. 용어의 효력

본 규격에서 사용된 다음의 용어들은 인증기관 및 가입자 소프트웨어의 구현 정도를 의미하는 것으로 [RFC2119]를 준용하며 다음과 같은 의미를 지닌다.

1) 해야한다, 필수이다, 강제한다 (기호 : M)

반드시 준수해야 한다.

2) 권고한다 (기호 : R)

보안성 및 상호연동을 고려하여 준수할 것을 권장한다.

3) 할 수 있다, 쓸 수 있다 (기호 : O)

주어진 상황을 고려하여 필요한 경우에 한해 선택적으로 사용할 수 있다.

4) 권고하지 않는다 (기호 : NR)

보안성 및 상호연동을 고려하여 사용하지 말 것을 권장한다.

5) 금지한다, 허용하지 않는다 (기호 : X)

반드시 사용하지 않아야 한다.

6) 언급하지 않는다, 정의하지 않는다 (기호 : -)

준수 여부에 대해 기술하지 않는다.

5. 인증서 프로파일

5.1. 인증서 기본필드

인증서 기본필드는 인증서의 버전, 발급자, 유효기간 등 인증서의 기본 정보를 나타낸다. 아래 정의된 기본필드는 공인인증서에 모두 포함되어야 한다.

5.1.1. 버전(Version)

버전 필드는 인증서 형식을 구별할 수 있는 기능을 제공하는데 본 규격에서는 정수 2값을 갖는 버전 3 인증서만 허용한다.

5.1.2. 일련 번호(Serial Number)

일련 번호 필드는 인증기관이 발급하는 공인인증서에 부여하는 유일한 양의 정수이다. 이 값은 인증서 효력정지 및 폐지목록에서 더 이상 유효하지 않는 목록들에 대한 참조정보로 사용된다.

5.1.3. 서명 알고리즘(Signature)

서명 알고리즘 필드는 인증기관이 인증서를 생성할 때 사용하는 서명 알고리즘의 OID 값을 가진다.

5.1.4. 발급자(Issuer)

발급자 필드는 인증서를 발급한 인증기관의 명칭을 DN 형식으로 표현하며 반드시 값을 가져야 한다.

5.1.5. 유효기간(Validity)

유효 기간 필드는 인증기관이 공인인증서의 상태를 보증해주는 기간을 나타낸다. 이 필드는 다음과 같이 인증서 유효기간의 시작을 나타내는 시작시각(notBefore)과 유효기간의 종료시점을 나타내는 종료시각(notAfter)에 시작 정보를 저장하여 유효기간을 표현한다.

5.1.6. 주체(Subject)

주체 필드는 인증서 주체의 명칭을 DN 형식으로 표현하며 반드시 값을 가져야 한다.

5.1.7. 공개키(Public Key)

소유자 공개키 필드는 소유자의 공개키에 대한 정보를 나타낸다.

5.2. 인증서 확장필드

5.2.1. 기관 키 식별자(Authority Key Identifier)

기관 키 식별자 확장필드는 인증서를 서명하는데 사용된 인증기관 개인키에 대응되는 공개키를 식별하기 위해 사용된다.

5.2.2. 주체 키 식별자(Subject Key Identifier)

주체 키 식별자 확장필드는 인증기관으로부터 인증 받은 공개키를 식별한다.

5.2.3. 키 사용(Key Usage)

키 사용 확장필드는 인증서에 포함된 소유자의 공개키가 사용되는 목적을 명시한다.

5.2.4. 인증서 정책(Certificate Policy)

인증서 정책 확장필드는 인증서를 발급하는데 적용된 인증기관의 인증서 정책을 나타낸다.

5.2.5. 주체 대체 이름(Subject Alternative Name)

주체 대체 이름 확장필드는 소유자의 추가적인 명칭을 나타내며, 인증서비스 영역 내에서 사용되는 고유한 식별정보를 나타낼 수 있다.

5.2.6. 기본 제한(Basic Constraints)

기본 제한 확장필드는 사용자가 인증기관의 역할을 수행하는 것을 방지하며 이를 위하여 인증기관의 여부 및 인증 경로의 길이를 제한한다. 이 확장필드는 인증기관용 인증서에만 포함되며 사용자 인증서에는 포함되지 말아야 한다.

5.2.7. 정책 제한 조건(Policy Constraints)

정책 제한 조건 확장필드는 인증서 정책 검사의 요구 및 인증서 정책 매핑에 대한 금지 등에 대한 정보를 나타낸다.

5.2.8. 확장된 키 사용(Extended Key Usage)

확장된 키 사용 확장필드는 키 사용목적 확장필드에서 나타낼 수 있는 것 이외의 공개키 사용목적을 명시한다.

5.2.9. CRL 배포 지점(CRL Distribution Points)

CRL 배포 지점 확장필드는 인증서의 상태정보를 확인하는 방법으로 인증서 효력정지 및 폐지목록을 사용하는 경우에 이를 획득할 수 있는 디렉토리 서버의 위치 정보를 나타낸다.

5.2.10. 기관 정보 액세스(Authority Information Access)

기관 정보 엑세스 확장필드는 인증서를 발급한 인증기관에 대한 정보를 획득하고자 하는 경우에 사용되며 인증기관 정보에 접근하는 방법 및 위치정보 등을 포함한다.

6. 인증서 효력정지 및 폐지목록 프로파일

6.1. 인증서 폐지목록 기본 필드

기본필드는 인증서 효력정지 및 폐지목록의 버전, 발급자, 발급일자 등의 기본 정보를 나타낸다.

6.1.1. 버전(Version)

버전 필드는 인코딩되는 인증서 효력정지 및 폐지 목록의 버전을 나타낸다.

6.1.2. 서명 알고리즘(Signature)

서명 알고리즘 필드는 공인인증기관이 인증서 효력정지 및 폐지목록을 생성할 때 사용하는 서명 알고리즘의 OID 값을 가진다.

6.1.3. 발급자(Issuer)

발급자 필드는 인증서 효력정지 및 폐지 목록을 발급한 기관의 명칭을 DN 형식으로 표현하며 반드시 값을 가져야 한다.

6.1.4. 게시 날짜(This Update)

게시 날짜 필드는 인증서 효력정지 및 폐지목록이 기관에서 발급된 시점을 나타낸다.

6.1.5. 다음 업데이트(Next Update)

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

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

6.1.6. 해지된 인증서(Revoked Certificates)

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

6.2. 인증서 폐지목록 확장 필드

6.2.1. 기관 키 식별자(Authority Key Identifier)

기관 키 식별자 확장필드는 인증서 효력정지 및 폐지목록 발급자의 인증서에 대한 공개키를 식별하기 위해 사용된다.

6.2.2. CRL 숫자(CRL Number)

CRL 숫자 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.

6.2.3. 배포 지점 발급 지점(Issuing Distribution Point)

배포 지점 발급 지점 확장필드는 해당 인증서 효력정지 및 폐지 목록을 획득할 수 있는 위치 정보를 포함한다.

7. 부록

7.1. 최상위 인증기관 인증서 프로파일

기본 필드 명	선택여부		입력 값
	생성	처리	
버전(Version)	m	m	V3
일련 번호(Serial Number)	m	m	고유일련번호(up to 20Byte)
서명 알고리즘(Signature)	m	m	sha256RSA
발급자 (Issuer)	m	m	CN = KICA_ROOT_CA OU = AccreditedCA O = Korea Information Certificate Authority C = KR
유효기간(Validity)	m	m	인증서 유효기간
주체(Subject)	m	m	CN = KICA_ROOT_CA OU = AccreditedCA O = Korea Information Certificate Authority

			C = KR
공개 키(Subject Public Key Info)	m	m	사용자 공개키에 대한 정보
확장필드(Extensions)	m	m	아래참조

확장필드	Critical	선택여부		입력값
		생성	처리	
주체 키 식별자 (Subject Key Identifier)	n	m	m	사용자의 공개키 hash값
키 사용 (Key Usage)	n	m	m	Certificate Signing Off-line CRL Signing CRL Signing (06)
기본 제한 (Basic Constraints)	c	m	m	Subject Type=CA Path Length Constraint=None
정책 제약 조건 (Policy Constraints)	c	o	m	Required Explicit Policy Skip Certs=0

c : critical, n : non-critical, m : 생성, o : 선택 , x : 생성하지 않음

7.2. 인증기관 인증서 프로파일

기본 필드 명	선택여부		입력 값
	생성	처리	
버전(Version)	m	m	V3
일련 번호(Serial Number)	m	m	고유일련번호(up to 20Byte)
서명 알고리즘(Signature)	m	m	sha256RSA
발급자 (Issuer)	m	m	CN = KICA_ROOT_CA OU = AccreditedCA

			O = Korea Information Certificate Authority C = KR
유효기간(Validity)	m	m	인증서 유효기간
주체(Subject)	m	m	CN = KICA_Signing_CA OU = AccreditedCA O = Korea Information Certificate Authority C = KR
공개 키(Subject Public Key Info)	m	m	사용자 공개키에 대한 정보
확장필드(Extensions)	m	m	아래참조

확장필드	Critical	선택여부		입력값
		생성	처리	
기관 키 식별자 (Authority Key Identifier)	n	m	m	발급기관의 공개키 hash값 인증기관 인증서의 발급자 DN 인증기관 인증서의 일련번호
주체 키 식별자 (Subject Key Identifier)	n	m	m	사용자의 공개키 hash값
키 사용 (Key Usage)	c	m	m	Certificate Signing Off-line CRL Signing CRL Signing (06)
인증서 정책 (Certificate Policies)	c	m	m	[1]Certificate Policy: Policy Identifier=모든 발급 정책 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.signgate.com/cps_signca.html

				[1,2]Policy Qualifier Info: Policy Qualifier Id=사용자 알림 Qualifier: Notice Text=Notice Text=This certificate is issued from Korea Information Certificate Authority Inc.(KICA_Root_CA)
기본 제한 (Basic Constraints)	c	m	m	Subject Type=CA Path Length Constraint=0
정책 제약 조건 (Policy Constraints)	c	m	m	Required Explicit Policy Skip Certs=0
확장된 키 사용 (Extended Key Usage)	n	o	m	문서 서명 (1.3.6.1.4.1.311.10.3.12)-
CRL 배포 지점 (CRL Distribution Points)	n	m	m	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://signca.signgate.com:389/cn=KICA_ROOT_CA,ou=AccreditedCA,o=Korea Information Certificate Authority,c=KR?authorityRevocationList
기관 정보 액세스 (Authority Information Access)	n	o	m	[1]Authority Info Access Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://signocsp.signgate.com:9020/OCSPServer

7.3. OCSP 인증서 프로파일

기본 필드 명	선택여부		입력 값
	생성	처리	
버전(Version)	m	m	V3
일련 번호(Serial Number)	m	m	고유일련번호(up to 20Byte)
서명 알고리즘(Signature)	m	m	sha256RSA
발급자 (Issuer)	m	m	CN = KICA_ROOT_CA OU = AccreditedCA O = Korea Information Certificate Authority C = KR
유효기간(Validity)	m	m	인증서 유효기간
주체(Subject)	m	m	CN = KICA_Signing_OCSP OU = AccreditedCA O = Korea Information Certificate Authority C = KR
공개 키(Subject Public Key Info)	m	m	공개키에 대한 정보
확장필드(Extensions)	m	m	아래참조

확장필드	Critical	선택여부		입력값
		생성	처리	
기관 키 식별자 (Authority Key Identifier)	n	m	m	발급기관의 공개키 hash값 인증기관 인증서의 발급자 DN 인증기관 인증서의 일련번호
주체 키 식별자	n	m	m	사용자의 공개키 hash값

(Subject Key Identifier)				
키 사용 (Key Usage)	c	m	m	Certificate Signing Off-line CRL Signing CRL Signing (06)
인증서 정책 (Certificate Policies)	c	m	m	[1]Certificate Policy: Policy Identifier=인증기관 정책 OID [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://trust.signgate.com [1,2]Policy Qualifier Info: Policy Qualifier Id=사용자 알림 Qualifier: Notice Text=This certificate is issued from Korea Information Certificate Authority Inc.(KICA_Root_CA)
기본 제한 (Basic Constraints)	c	m	m	Subject Type=CA Path Length Constraint=0
정책 제약 조건 (Policy Constraints)	c	m	m	Required Explicit Policy Skip Certs=0
확장된 키 사용 (Extended Key Usage)	c	o	m	OCSP 서명 (1.3.6.1.5.5.7.3.9)
CRL 배포 지점 (CRL Distribution Points)	n	m	m	[1]CRL Distribution Point Distribution Point Name:

				Full Name: URL=ldap://signca.signgate.com:389/cn=KICA_ROOT_CA,ou=AccreditedCA,o=Korea Information Certificate Authority,c=KR?authorityRevocationList
기관 정보 액세스 (Authority Information Access)	n	o	m	[1]Authority Info Access Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://signocsp.signgate.com:9020/OCSPServer

7.4. TSA 인증서 프로파일

기본 필드 명	선택여부		입력 값
	생성	처리	
버전(Version)	m	m	V3
일련 번호(Serial Number)	m	m	고유일련번호(up to 20Byte)
서명 알고리즘(Signature)	m	m	sha256RSA
발급자 (Issuer)	m	m	CN = KICA_ROOT_CA OU = AccreditedCA O = Korea Information Certificate Authority C = KR
유효기간(Validity)	m	m	인증서 유효기간
주체(Subject)	m	m	CN = KICA_Signing_TSA

			OU = AccreditedCA O = Korea Information Certificate Authority C = KR
공개 키(Subject Public Key Info)	m	m	공개키에 대한 정보
확장필드(Extensions)	m	m	아래참조

확장필드	Critical	선택여부		입력값
		생성	처리	
기관 키 식별자 (Authority Key Identifier)	n	m	m	발급기관의 공개키 hash값 인증기관 인증서의 발급자 DN 인증기관 인증서의 일련번호
주체 키 식별자 (Subject Key Identifier)	n	m	m	사용자의 공개키 hash값
키 사용 (Key Usage)	c	m	m	Certificate Signing Off-line CRL Signing CRL Signing (06)
인증서 정책 (Certificate Policies)	c	m	m	[1]Certificate Policy: Policy Identifier=인증기관 정책 OID [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://trust.signgate.com [1,2]Policy Qualifier Info: Policy Qualifier Id=사용자 알림

				Qualifier: Notice Text=This certificate is issued from Korea Information Certificate Authority Inc.(KICA_Root_CA)
기본 제한 (Basic Constraints)	c	m	m	Subject Type=CA Path Length Constraint=0
정책 제약 조건 (Policy Constraints)	c	m	m	Required Explicit Policy Skip Certs=0-
확장된 키 사용 (Extended Key Usage)	c	o	m	타임스탬프 (1.3.6.1.5.5.7.3.8)-
CRL 배포 지점 (CRL Distribution Points)	n	m	m	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://signca.signgate.com:389/cn=KICA_ROOT_CA,ou=AccreditedCA,o=Korea Information Certificate Authority,c=KR?authorityRevocationList
기관 정보 액세스 (Authority Information Access)	n	o	m	[1]Authority Info Access Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://signocsp.signgate.com:9020/OCSPServer

7.5. 가입자 인증서 프로파일

기본 필드 명	선택여부	입력 값

	생성	처리	
버전(Version)	m	m	V3
일련 번호(Serial Number)	m	m	고유일련번호(up to 20Byte)
서명 알고리즘(Signature)	m	m	sha256RSA
발급자 (Issuer)	m	m	CN = KICA_Signing_CA OU = AccreditedCA O = Korea Information Certificate Authority C = KR
유효기간(Validity)	m	m	인증서 유효기간
주체(Subject)	m	m	CN = 사용자명 OU = 업체명 OU = AccreditedCA O = Korea Information Certificate Authority C = KR
공개 키(Subject Public Key Info)	m	m	사용자 공개키에 대한 정보
확장필드(Extensions)	m	m	아래참조

확장필드	Critical	선택여부		입력값
		생성	처리	
기관 키 식별자 (Authority Key Identifier)	n	m	m	발급기관의 공개키 hash값
주체 키 식별자 (Subject Key Identifier)	n	m	m	사용자의 공개키 hash값
키 사용 (Key Usage)	c	m	m	Digital Signature Non-Repudiation

인증서 정책 (Certificate Policies)	c	m	m	[1]Certificate Policy: Policy Identifier=인증기관 정책 OID [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://trust.signgate.com [1,2]Policy Qualifier Info: Policy Qualifier Id=사용자 알림 Qualifier: Notice Text= This certificate is issued from Korea Information Certificate Authority Inc.(KICA Signing CA)
주체 대체 이름 (Subject Alternative Name)	n	m	m	Other Name = EVID
기본 제한 (Basic Constraints)	n	x	x	Subject Type=End Entity Path Length Constraint=None
확장된 키 사용 (Extended Key Usage)	n	o	o	문서 서명 (1.3.6.1.4.1.311.10.3.12) 전자 메일 보안 (1.3.6.1.5.5.7.3.4)
CRL 배포 지점 (CRL Distribution Points)	n	m	m	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://signds.signgate.com:389/ou=해당dp,ou=crl,ou=AccreditedCA,o=Korea Information Certificate Authority,c=KR
기관 정보 액세스 (Authority Information Access)	n	m	m	[1]Authority Info Access Access Method=온라인 인증서 상태 프로토콜 (1.3.6.1.5.5.7.48.1) Alternative Name:

				URL=http://signocsp.signgate.com:9020/OCSPServer

7.6. 가입자 인증서 프로파일(싸인오케이서비스)

기본 필드 명	선택여부		입력 값
	생성	처리	
버전(Version)	m	m	V3
일련 번호(Serial Number)	m	m	고유일련번호(up to 20Byte)
서명 알고리즘(Signature)	m	m	sha256RSA
발급자 (Issuer)	m	m	CN = KICA_Signing_CA OU = AccreditedCA O = Korea Information Certificate Authority C = KR
유효기간(Validity)	m	m	인증서 유효기간
주체(Subject)	m	m	CN = 사용자명 OU = 업체명 OU = licensedCA O = KICA C = KR
공개 키(Subject Public Key Info)	m	m	사용자 공개키에 대한 정보
확장필드(Extensions)	m	m	아래참조

확장필드	Critical	선택여부		입력값
		생성	처리	
기관 키 식별자 (Authority Key Identifier)	n	m	m	발급기관의 공개키 hash값

주체 키 식별자 (Subject Key Identifier)	n	m	m	사용자의 공개키 hash값
키 사용 (Key Usage)	c	m	m	Digital Signature Non-Repudiation
인증서 정책 (Certificate Policies)	c	m	m	[1]Certificate Policy: Policy Identifier=인증기관 정책 OID [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://trust.signgate.com [1,2]Policy Qualifier Info: Policy Qualifier Id=사용자 알림 Qualifier: Notice Text= This certificate is issued from Korea Information Certificate Authority Inc.(KICA Signing CA)
주체 대체 이름 (Subject Alternative Name)	n	m	m	Other Name = EVID
기본 제한 (Basic Constraints)	n	x	x	Subject Type=End Entity Path Length Constraint=None
확장된 키 사용 (Extended Key Usage)	n	o	o	
CRL 배포 지점 (CRL Distribution Points)	n	m	m	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=ldap://signds.signgate.com:389/ou=해당dp,ou=crl,ou=AccreditedCA,o=Korea Information Certificate

				Authority,c=KR
기관 정보 액세스 (Authority Information Access)	n	m	m	[1]Authority Info Access Access Method=온라인 인증서 상태 프로토콜(1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://signocsp.signgate.com:9020/OCSPServer

7.7. 인증기관 인증서 폐지목록(ARL) 프로파일

기본 필드 명	생성	처리	입력 값
버전(Version)	m	m	V2
서명 알고리즘(Signature)	m	m	sha256RSA
발급자 (Issuer Name)	m	m	CN = KICA_Root_CA OU = AccreditedCA O = KICA C = KR
게시 날짜(This Update)	m	m	게시 날짜
다음 업데이트(Next Update)	m	m	만료 날짜 (유효기간: 100일)
해지된 인증서 -일련번호 -해지 날짜 -CRL 엔트리 확장필드	- m m m	- m m m	제공됨 (목록이 없는 경우 값이 없음) 폐지된 인증서의 일련번호 입력 폐지날짜 입력 아래 참고
CRL 확장필드(CRL Extensions)	m	m	아래 참고

인증서 효력정지 및 폐지 목록 확장필드 명	critical	선택여부		입력 값
		생성	처리	
기관 키 식별자(Authority Key Identifier)	n	m	m	발급기관의 공개키 hash값 인증기관 인증서의 발급자 DN 인증기관 인증서의 일련번호
CRL 숫자(CRL Number)	n	m	m	CRL 일련번호

7.8. 가입자 인증서 폐지목록(CRL) 프로파일

8. 기본 필드 명	생성	처리	입력 값
버전(Version)	m	m	V2
서명 알고리즘(Signature)	m	m	sha256RSA
발급자 (Issuer Name)	m	m	CN = KICA_Signing_CA OU = AccreditedCA O = KICA C = KR
게시 날짜(This Update)	m	m	게시 날짜
다음 업데이트(Next Update)	m	m	만료 날짜 (유효기간: 24시간)
해지된 인증서	-	-	제공됨 (목록이 없는 경우 값이 없음)
-일련번호	m	m	폐지된 인증서의 일련번호 입력
-해지 날짜	m	m	폐지날짜 입력
-CRL 엔트리 확장필드	m	m	아래 참고
CRL 확장필드(CRL Extensions)	m	m	아래 참고

인증서 효력정지 및 폐지 목록 확장필드명	critical	선택여부		입력 값
		생성	처리	
기관 키 식별자(Authority Key Identifier)	n	m	m	발급기관의 공개키 hash값 인증기관 인증서의 발급자 DN 인증기관 인증서의 일련번호
CRL 숫자(CRL Number)	n	m	m	CRL 일련번호