전자서명인증관리체계 DN 규격

Distinguished Name Specification

v1.21

2009년 9월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

목 차

전자서명인증관리체계 DN 규격
Distinguished Name Specification

1. 개 요

본 규격에서는 전자서명법 상에서 구축된 전자서명인증관리체계에서 공인인증기관이 제공하는 PKI 인증서비스의 상호연동을 위해 필수적으로 요구되는 DN 형식을 관련 표준 및 규격을 고려하여 규정한다.

2. 규격의 구성 및 범위

본 규격은 전자서명인증관리체계 공인인증기관 및 가입자 소프트웨어에서 이용자에게 호환성 있는 유·무선 PKI 인증서비스를 제공하는데 있어 필요한 DN의 기술적 요구사항을 명시하고 있으며 크게 두 부분으로 나뉘어 진다.

첫 번째로 공인인증서와 공인인증서 효력정지 및 폐지목록에 주로 사용되고 있는 전자서명인증관리체계 DN의 구성 및 속성에 대해 정의하였고 DN을 문자열로 표현하기 위한 규칙을 정의하였다.

두 번째로 부록에서는 전자서명인증관리체계 DN 속성값의 속성명, OID, 최대길이, 인코딩 타입 등의 정의와 생성·처리에 관한 요구사항 및 DN 구성 형식을 제시하고 있다.

3. 관련 표준 및 규격

3.1 국외 표준 및 규격

[X500] ITU-T Recommendation X.500 (2001) | ISO/IEC 9594-1:2001, *Information technology - Open Systems Interconnection - The Directory : Overview Of Concepts, Models and Services*

[X501] ITU-T Recommendation X.501 (2001) | ISO/IEC 9594-2:2001, *Information technology - Open Systems Interconnection - The*

Directory : Models

[X509] ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8:1998, *Information technology - Open Systems Interconnection - The Directory : Authentication Framework*

[X520] ITU-T Recommendation X.520 (2001) | ISO/IEC 9594-6:2001, *Information technology - Open Systems Interconnection - The Directory : Selected Attribute Types*

[RFC2119] IETF, RFC 2119, *Key Words for use in RFCs to Indicate Requirement Levels,* 1997

[RFC2247] IETF, RFC 2247, *Using Domains in LDAP/X.500 Distinguished Names,* 1998

[RFC2252] IETF, RFC 2252, *Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions,* 1997

[RFC2253] IETF, RFC 2253, *Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names,* 1997

[RFC2255] IETF, RFC 2255, *The LDAP URL Format,* 1997

[RFC2256] IETF, RFC 2256, *A Summary of the X.500(96) User Schema for use with LDAPv3,* 1997

[RFC3039] IETF, RFC 3039, *Internet X.509 Public Key Infrastructure Qualified Certificates Profile,* 2001

[RFC3280] IETF, RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile, 2002*

[PKCS9] RSA, PKCS#9 v2.0, *Selected Object Classes and Attribute Types,* 2000

[WAPCert] OMA, WAP-211-WAPCert-20010522-a, *WAP Certificate and CRL Profiles,* 2001

3.2 국내 표준 및 규격

[TTA-X509R2] TTA, TTAS.IT-X.509/R2, *디렉토리 시스템 인증 프레임워크 표준,* 2000

[KCAC.TS.CERTPROF] KISA, KCAC.TS.CERTPROF, v1.70, *전자서명 인증서 프로파일 규격,* 2009

[KCAC.TS.CRLPROF] KISA, KCAC.TS.CRLPROF, v1.50, *전자서명 인증서 효력정지 및 폐지목록 프로파일 규격*, 2009

3.3 기타

[ISTF-018] ISTF, ISTF-018, *공인인증기관간 상호연동을 위한 PKI 표준*, 2002, http://www.istf.or.kr

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) 공인인증서
다) 공인인증기관
라) 전자서명인증관리체계
마) 가입자
바) 이용자
사) 가입자 설비

4.2 용어의 정의

정의하지 않음

4.3 용어의 효력

본 규격에서 사용된 다음의 용어들은 공인인증기관 및 가입자 소프트웨어가 DN을 생성하거나 처리하는데 따라야 할 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 약어가 이용된다.

가) DN : Distinguished Name, 고유 이름
나) OID : Object Identifier, 객체 식별자
다) UTF8 : Universal Transformation Format, 8bit
라) ASN.1 : Abstract Syntax Notation One
마) RDN : Relative Distinguished Name

6. 전자서명인증관리체계 DN 구성 및 속성 정의

6.1 DN 구성

DN은 하나이상의 RDN이 순서를 가지고 구성되어야 한다. 각각의 RDN은 6.2에서 정의되는 속성을 준용해야 하며 DN의 ASN.1 형식은 다음과 같다.

```
Name :: CHOICE { rdnSequence RDNSequence }

RDNSequence ::= SEQUENCE OF RelativeDistinguishedName

DistinguishedName ::= RDNSequence

RelativeDistinguishedName ::= SET SIZE (1..MAX) OF
        AttributeTypeAndValue
```

```
AttributeTypeAndValue ::= SEQUENCE {
        type    AttributeType,
        value   AttributeValue }
```

6.2. DN 속성 정의

다음에서 정의한 DN 속성들의 ASN.1 형식은 별도로 언급하지 않는 한 [X.520] 또는 [RFC2256]을 따라야 하며 속성값의 최대길이는 “부록 1. 전자서명인증관리체계 DN 속성 정의”를 준용해야 한다.

각 속성에 대한 생성·처리는 “부록 2. 전자서명인증관리체계 DN 구성 속성별 생성·처리”를 준용해야 하며 부록 2. 에서 언급되지 않은 속성 사용은 허용하지 않는다.

6.2.1 Common Name

가입자의 이름을 나타내는 속성으로 약칭은 ‘CN’을 사용해야 하며 CN 값에 가입자 이름을 포함할 것을 권고한다.

```
commonName      ATTRIBUTE ::= {
        SUBTYPE OF              name
        WITH SYNTAX     DirectoryString {ub-common-name}
        ID                      id-at-commonName }
```

6.2.2 Surname

가입자 이름의 성을 나타내는 속성이며 약칭으로 ‘SN’을 사용해야 한다.

```
surName ATTRIBUTE ::= {
        SUBTYPE OF              name
        WITH SYNTAX     DirectoryString {ub-name}
        ID                      id-at-surName }
```

6.2.3 Serial Number

가입자를 구별하기 위한 속성으로 약칭에 대해서는 본 규격에서 정의하지 않는다.

```
serialNumber ATTRIBUTE ::= {
        WITH SYNTAX                 PrintableString(SIZE(1..ub-serialNumber))
        EQUALITY MATCHING RULE      caseIgnoreMatch
        SUBSTRING MATCHING RULE     caseIgnoreSubstringMatch
        ID                          id-at-serial-number }
```

6.2.4 Country Name

가입자가 속한 국가명을 나타내기 위한 속성이며 약칭으로 'C'를 사용해야 한다. 속성값은 ISO 3166 표준을 준용하여 반드시 PrintableString 두 글자로 표현해야 한다.

```
countryName ATTRIBUTE ::= {
        SUBTYPE OF                  name
        WITH SYNTAX                 PrintableString(SIZE(2))
                                    -- ISO 3166 code only
        SINGLE VALUE                TRUE
        SUBSTRING MATCHING RULE     caseIgnoreSubstringMatch
        ID                          id-at-countryName }
```

6.2.5 Locality Name

가입자가 속한 지역명을 나타내기 위한 속성이며 약칭으로 'L'을 사용해야 한다.

```
localityName ATTRIBUTE ::= {
        SUBTYPE OF          name
        WITH SYNTAX         DirectoryString{ub-locality-name}
        ID                  id-at-localityName }
```

6.2.6 State or Province Name

가입자가 속한 도시나 도명을 나타내기 위한 속성이며 약칭으로 'S' 또는 'ST'를 사용해야 한다.

```
stateOrProvinceName ATTRIBUTE ::= {
        SUBTYPE OF          name
        WITH SYNTAX         DirectoryString{ub-state-name}
```

```
        ID                          id-at-stateOrProvinceName }
```

6.2.7 Street Address

가입자가 거주하는 거리명 또는 번지수를 나타내기 위한 속성이며 약칭으로 'STREET'을 사용해야 한다.

```
streetAddress ATTRIBUTE ::= {
        WITHSYNTAX                  DirectoryString{ub-street-address}
        EQUALITY MATCHING RULE      caseIgnoreMatch
        SUBSTRING MATCHING RULE     caseIgnoreSubstringMatch
        ID                          id-at-streetAddress }
```

6.2.8 Organization Name

가입자가 속한 조직명을 나타내기 위한 속성이며 약칭으로 'O'를 사용해야 한다. 조직명을 단계적으로 나타내기 위한 경우 본 속성을 여러 번 사용할 수 있다.

```
organizationName ATTRIBUTE ::= {
        SUBTYPE OF          name
        WITH SYNTAX         DirectoryString {ub-organization-name}
        ID                  id-at-organizationName }
```

6.2.9 Organizational Unit Name

가입자가 속한 하위 조직명를 나타내기 위한 속성이며 약칭으로 'OU'를 사용해야 한다. 부서 조직이 계층적으로 몇 단계로 이루어지는 경우 본 속성을 여러 번 사용할 수 있다. 공인인증기관은 OU값으로 AccreditedCA를 사용해야 한다.

```
organizationalUnitName ATTRIBUTE ::= {
        SUBTYPE OF          name
        WITH SYNTAX         DirectoryString {ub-organizational-unit-name}
        ID                  id-at-organizationalUnitName }
```

6.2.10 Title

가입자가 속한 조직에서의 직위를 나타내기 위한 속성이며 약칭으로 'T' 또는

‘TITLE’을 사용해야 한다.

```
title ATTRIBUTE ::= {
        SUBTYPE OF          name
        WITH SYNTAX         DirectoryString {ub-title}
        ID                  id-at-title }
```

6.2.11 Business Category

가입자가 종사하는 직업의 종류를 나타내기 위한 속성이며 약칭에 대해서는 본 규격에서 정의하지 않는다.

```
businessCategory ATTRIBUTE ::= {
        WITH SYNTAX                 DirectoryString {ub-business-category}
        EQUALITY MATCHING RULE      caseIgnoreMatch
        SUBSTRING MATCHING RULE     caseIgnoreSubstringMatch
        ID                          id-at-businessCategory }
```

6.2.12 Given name

가입자의 부가적인 이름을 나타내는 속성이며 약칭으로 ‘G’ 또는 ‘GIVENNAME’을 사용해야 한다.

```
givenName ATTRIBUTE ::= {
        SUBTYPE OF                  name
        WITH SYNTAX                 DirectoryString {ub-name}
        ID                          id-at-givenName }
```

6.2.13 Initials

가입자 이름의 약어를 나타내는 속성이며 약칭으로 ‘I’ 또는 ‘INITIALS’를 사용해야 한다.

```
initials ATTRIBUTE ::= {
        SUBTYPE OF                  name
        WITH SYNTAX                 DirectoryString {ub-name}
        ID                          id-at-givenName }
```

6.2.14 Generation Qualifier

가입자 이름의 접미어를 나타내는 속성이며 약칭에 대해서는 본 규격에서 정의하지 않는다.

```
generationQualifier ATTRIBUTE ::= {
        SUBTYPE OF                  name
        WITH SYNTAX                 DirectoryString {ub-name}
        ID                          id-at-generationQualifier }
```

6.2.15 Unique Identifier

가입자 DN이 재 사용될 경우 이를 구별하기 위한 속성으로 약칭에 대해서는 본 규격에서 정의하지 않는다. 객체 식별자, 인증서, 날짜, 타임스탬프 등이 속성 값으로 사용될 수 있다.

```
uniqueIdentifier ATTRIBUTE ::= {
        WITH SYNTAX                     UniqueIdentifier
        EQUALITY MATCHING RULE          bitStringMatch
        ID                              id-at-uniqueIdentifier }
UniqueIdentifier            ::=         BIT STRING
```

6.2.16 DN Qualifier

가입자의 RDN를 구별하기 위한 속성으로 약칭에 대해서는 본 규격에서 정의하지 않는다.

```
dnQualifier ATTRIBUTE ::= {
        WITH SYNTAX                     PrintableString
        EQUALITY MATCHING RULE          caseIgnoreMatch
        ORDERING MATCHING RULE          caseIgnoreOrderingMatch
        SUBSTRING MATCHING RULE         caseIgnoreSubstringMatch
        ID                              id-at-dnQualifier }
```

6.2.17 Pseudonym

가입자의 필명이나 익명을 나타내기 위한 속성이며 약칭에 대해서는 본 규격에서 정의하지 않는다. 다음에 기술된 본 속성의 ASN.1 표현은 [RFC3039]를 준용해야 한다.

```
pseudonym ATTRIBUTE ::= {
        WITH SYNTAX         DirectoryString { ub-name }
        ID                  id-at-pseudonym }
```

6.2.18 Domain Component

가입자의 도메인 주소를 나타내기 위한 속성이며 약칭으로 DC을 사용해야 한다. 본 규격에 기술된 DC의 정의 및 문자열 표현형식은 [RFC2247]을 준용해야 한다.

```
(
        0.9.2342.19200300.100.1.25
        NAME 'dc'
        EQUALITY caseIgnoreIA5Match
        SUBSTR caseIgnoreIA5SubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26
        SINGLE-VALUE
)
```

6.2.19 emailAddress

가입자의 E-mail 주소를 나타내기 위한 속성이며 약칭으로 'E'를 사용해야 한다. 아래의 속성 형식은 [PKCS9] 표준에서 기술된 형식과 동일하다.

```
emailAddress ATTRIBUTE ::= {
        WITH SYNTAX                 IA5String (SIZE (1..pkcs-9-ub-emailAddress))
        EQUALITY MATCHING RULE      pkcs9CaseIgnoreMatch
        ID                          pkcs-9-at-emailAddress
}
```

6.2.20 rfc822MailBox

가입자의 E-mail 주소를 나타내기 위한 속성이며 약칭에 대해서는 본 규격에서 정의하지 않는다.

```
rfc822Mailbox ATTRIBUTE ::= {
```

WITH SYNTAX	Ia5String (SIZE (1..ub-rfc822-mailbox))
EQUALITY MATCHING RULE	caseIgnoreIa5Match
SUBSTRING MATCHING RULE	caseIgnoreIa5SubstringsMatch
ID	id-rfc822Mailbox }

7. 전자서명인증관리체계 DN 문자열 표현 규칙

DN의 문자열 표현시 각각의 RDN은 ‘,’로 구분된다. 하나의 RDN은 속성타입과 속성값으로 표현되며 ‘속성타입 = 속성값’과 같이 ‘=’로 연결된다. 만일 multi-valued RDN을 사용하는 경우에는 “OU=Sales+CN=J"와 같이 각각의 속성타입과 속성값이 ‘+’로 결합되어야 한다.

속성타입은 부록 1.에서 정의된 속성약칭을 사용하며 속성약칭이 정의되지 않은 속성타입은 속성명을 사용해야 한다.

DN의 문자열 표현시 RDN 속성값은 [RFC2253]을 준용하여 UTF8 스트링으로 표현해야 한다. “CN=John, Smith"와 같이 DN 값에 특수문자(,)를 포함하는 경우에는 ”CN=John₩, Smith"처럼 '₩'를 특수문자 앞에 명시하여 escape 처리해야 한다.

부록 1. 전자서명인증관리체계 DN 속성정의

속성명	OID	속성 약칭[1]	최대[2] 길이	ASN.1 스트링 타입
commonName	{id-at 3}	CN	64	DirectoryString
surName	{id-at 4}	SN	64	DirectoryString
serialNumber	{id-at 5}	-	64	PrintableString
countryName	{id-at 6}	C	2	PrintableString(SIZE(2))
localityName	{id-at 7}	L	128	DirectoryString
stateOrProvinceName	{id-at 8}	S/ST	128	DirectoryString
streetAddress	{id-at 9}	STREET	128	DirectoryString
organizationName	{id-at 10}	O	64	DirectoryString
organizationalUnitName	{id-at 11}	OU	64	DirectoryString
title	{id-at 12}	T/TITLE	64	DirectoryString
businessCategory	{id-at 15}	-	128	DirectoryString
givenName	{id-at 42}	G/GIVENNAME	64	DirectoryString
initials	{id-at 43}	I/INITIALS	64	DirectoryString
generationQualifier	{id-at 44}	-	64	DirectoryString
uniqueIdentifier	{id-at 45}	-	64	BIT STRING
dnQualifier	{id-at 46}	-	64	PrintableString
pseudonym	{id-at 65}	-	64	DirectoryString
domainComponent	0.9.2342.19200300.100.1.25	DC	64	IA5String
emailAddress	1.2.840.113549.1.9.1	E	128	IA5String
rfc822MailBox	0.9.2342.19200300.100.1.3	-	128	IA5String
- : Not Defined				

1) 속성 약칭은 대소문자를 구분하지 않음
2) DN의 최대길이는 256 바이트로 권고함
3) DirectoryString으로 표현되는 DN 속성값은 [RFC3280]을 준용하여 2003년 12월 31일 이후에는 해당 속성값을 UTF8 스트링(UTF8 String)으로 표현함

※ id-at OBJECT IDENTIFIER::= {joint-iso-itu(2) ds(5) attribute(4)}

부록 2. 전자서명인증관리체계 DN 속성별 생성·처리

속성명	인증서 생성				인증서 처리
	전자서명인증관리센터	공인인증기관	가입자		
			법인	개인	
commonName	M	R	R	M	M
surName	×	×	×	×	R
serialNumber	O	O	O	O	M
countryName	M	M	M	M	M
localityName	O	O	O	O	M
stateOrProvinceName	O	O	O	O	M
streetAddress	O	O	O	O	M
organizationName	M	M	M	M	M
organizationalUnitName	M	M	R	R	M
title	×	×	×	×	R
businessCategory	×	×	×	×	O
givenName	×	×	×	×	R
initials	×	×	×	×	R
generationQualifier	×	×	×	×	R
uniqueIdentifier	×	×	×	×	O
dnQualifier	R	R	R	R	M
pseudonym	×	×	×	×	R
domainComponent	O	O	R	O	M
emailAddress	NR	NR	NR	NR	M
rfc822MailBox	×	×	×	×	O

※ M : 필수, R : 권고, O : 선택, × : 금지, NR : 권고하지 않음

부록 3. 전자서명인증관리체계 DN 구성 형식

□ 전자서명 인증관리센터

o C=KR, O=KISA, OU={Korea Certification Authority Central}, CN={KISA RootCA 2}

□ 공인인증기관

o C=KR,O=공인인증기관명[1],OU=AccreditedCA,[CN], [domainComponent]

□ 법인용 가입자

o C=KR, O=공인인증기관명[1], [OU={Sales, OU=전자거래}], [CN={가입자이름[2]}], [DC={www, DC=Sales, DC=.com}]

□ 개인용 가입자

o C=KR, O=공인인증기관명[1], [OU={AccreditedCA}], CN={가입자이름[2]}, [E={admin@aaa.co.kr}]

1) 공인인증기관명 = 영문공인서비스명 또는 영문공인인증기관명

2) 가입자이름 = 전자서명법시행규칙 제13조의3에 명시된 신원확인증표상의 이름

※ [ ] : 권고, { } : 예시, | : 선택, ( ) : 병기

※ 각 속성에 대한 순서는 위의 예를 따른다.

부록 4. 규격 연혁

버전	제·개정일	제·개정내역
v1.00	2000년 2월	· "전자서명 인증서 DN 규격"으로 제정
v1.10	2003년 5월	· 무선 전자서명인증서 DN 규격 v1.21 흡수 통합 · 전체적인 문서 형식 및 구성을 전자서명인증관리체계 규격 문서양식에 맞게 개정 · 2.가. 속성 정의를 부록 1, 부록 전자서명인증관리체계 DN 속성 정의, 부록 2. 전자서명인증관리체계 DN 생성·처리로 개정 · 2.나. DN 사용방법을 부록 3. 전자서명인증관리체계 DN 구성 형식으로 개정 · 3. 국·내외 DN 규격 현황 비교 삭제 · 6장 전자서명인증관리체계 DN 구성 및 속성 정의 · 7장 전자서명인증관리체계 DN 문자열 표현 규칙 정의 · 붙임 1. DN 국제표준 규격 현황 삭제 · 참고사항 삭제
v1.11	2007년 4월	· stateOrProvinceName의 약자로 'ST'추가 · streetName의 약자로 'STREET'만 사용하도록 변경
v1.20	2008년 10월	· 관련 국내 표준 및 규격 갱신 내용 반영 · 법률 공포번호가 해당 법률 개정시마다 변경되는 점을 고려하여 법령명으로 개정
v1.21	2009년 9월	· 공인전자서명인증체계 기술규격 개정에 따라 본문 내용 중 관련 기술규격 참조 변경 사항 개정