# 공인인증서 경로검증 기술규격

# Accredited Certificate Path Validation Specification

v1.11

2009년 9월

KISA 한국인터넷진흥원
Korea Internet & Security Agency

# 목 차

# 표 목 차

# 그 림 목 차

# 공인인증서 경로검증 기술규격

Accredited Certificate Path Validation Specification

## 1. 개 요

전자서명인증체계 공인인증서비스의 신뢰성을 보장하기 위해 공인인증서(이하 인증서) 검증 절차에 관한 규격의 제정 및 개발이 필요하다. 따라서, 본 규격에서는 인증서를 검증하기 위한 인증경로 구축 방법과 검증 절차를 명시한다.

## 2. 규격의 구성 및 범위

본 규격은 인증서 검증 알고리즘을 인증서 경로구축과 인증서 경로검증 알고리즘으로 나누어 명시한다.

첫 번째로, 인증서 경로구축은 인증서 경로검증의 한 과정으로 인증서를 검증하기 위해 필요한 인증경로를 구축하는 절차를 명시한다.

두 번째로, 인증서 경로검증 알고리즘은 인증경로 상의 인증서를 검증하는 절차를 명시한다. 인증서 검증 절차에는 서명 검증, 인증서 상태 검증, 유효기간 검증, 정책 검증 등이 포함된다.

## 3. 관련 표준 및 규격

### 3.1 국외 표준 및 규격

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

[RFC2459] IETF, RFC2459, *Internet X.509 Punlic Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile,*

January 1999

[RFC2510] IETF, RFC2510, *Internet X.509 Punlic Key Infrastructure Certificate Management Protocols,* March 1999

[RFC3280] IETF, RFC3280, *Internet X.509 Punlic Key Infrastructure Certificate and Certificate Revocation List(CRL) Profile,* April 2002

[RFC2119] IETF, RFC2119, *Key words for use in RFCs to Indicate Requirement Levels,* March 1997

## 3.2 국내 표준 및 규격

[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

[TTA-X509/R2] TTA, TTAS.IT-X.509/R2, *디렉토리 시스템 인증 프레임워크 표준,* 2000

[KCAC.TS.DN] KISA, KCAC.TS.DN, v1.21, *전자서명인증체계 DN 규격,* 2009

[KCAC.TS.SIVID] KISA, KCAC.TS.SIVID, v1.21, *식별번호를 이용한 본인확인 기술규격,* 2009

[KCAC.TS.OCSP] KISA, KCAC.TS.OCSP, v1.21, *실시간 인증서 상태확인 기술규격,* 2009

[KCAC.TS.CTL] KISA, KCAC.TS.CTL, v1.40, *인증기관간 상호연동을 위한 CTL 기술규격,* 2009

[KCAC.TS.UI] KISA, KCAC.TS.UI, v1.80, *공인인증기관간 상호연동을 위한 사용자 인터페이스 기술규격,* 2009

[KCAC.TS.ACUG] KISA, KCAC.TS.ACUG, v1.11, *전자서명인증체계 공인인증서 갱신 규격,* 2009

## 3.3 기타

[KCAC.TG.OID] KISA, KCAC.TG.OID, v1.30, *전자서명인증체계 OID 가이드라인,* 2008

# 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

## 4.2 용어의 정의

본 규격을 위하여 다음과 같은 용어들을 정의한다.

가) 대상인증서 : 검증대상이 되는 인증서
나) 신뢰당사자 : 대상인증서의 신뢰성을 확인하기 위해 인증서 검증을 수행하는 자
다) 최상위인증기관정보 : 신뢰당사자가 [KCAC.TS.UI] 및 [KCAC.TS.ACUG]에서 정의한 최상위 인증기관 인증서의 신뢰여부 확인을 통하여 신뢰하는 정보로 자가서명된 인증서 형태로 구성됨

## 4.3 용어의 효력

본 규격에서 사용된 다음의 용어들은 전자서명인증체계 공인인증서 경로검증 알고리즘의 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, 식별명칭
나) CRL : Certificate Revocation List, 인증서 효력정지 및 폐지목록
다) AKI : Authority Key Identifier, 발급자 공개키 식별자
라) SKI : Subject Key Identifier, 소유자 공개키 식별자
마) SAN : Subject Alternative Name, 소유자 대체 명칭
바) CP : CP, 인증서 정책
사) CRLDP : CRL Distribution Point, 인증서 효력정지 및 폐지목록 분배점
아) AIA : Authority Information Access, 발급자 정보 접근
자) IDP : Issuing Distribution Point, 인증서 효력정지 및 폐지목록 발급 분배점

## 6. 인증 경로구축

신뢰당사자는 인증서를 검증하기 위해서 대상인증서로부터 최상위인증기관 정보까지의 인증 경로를 구축해야 한다.

신뢰당사자가 온라인으로 저장소를 이용하여 최상위인증기관인정보까지의 인증 경로를 구축하는 경우, 대상인증서의 AIA 필드의 id-ad-caIssuers 정보를 이용해야 한다.

신뢰당사자는 하위인증서의 AKI 확장필드 내에 포함된 keyIdentifier와 authorityCertIssuer 및 authorityCertSerialNumber가 상위인증서의 SKI 확장필드에 포함된 keyIdentifier와 상위인증서의 발급자 DN 및 인증서 일련번호와 일치하는지를 검증해야 한다.

DN의 일치성을 확인할 때 다음의 규칙을 적용해야 한다.

- 다른 인코딩 형식(예: PrintableString과 BMPString)으로 인코딩 된 속성 값은 다른 문자로 인식한다
- PrintableString이 아닌 다른 인코딩 형식으로 인코딩 된 속성 값은 대·

소문자를 구분한다 (바이너리 비교방식)

o PrintableString 인코딩 형식으로 인코딩 된 속성 값은 대·소문자를 구분하지 않는다 (예: “Marianne Swanson”은 “MARIANNE SWANSON"과 동일한 문자열)

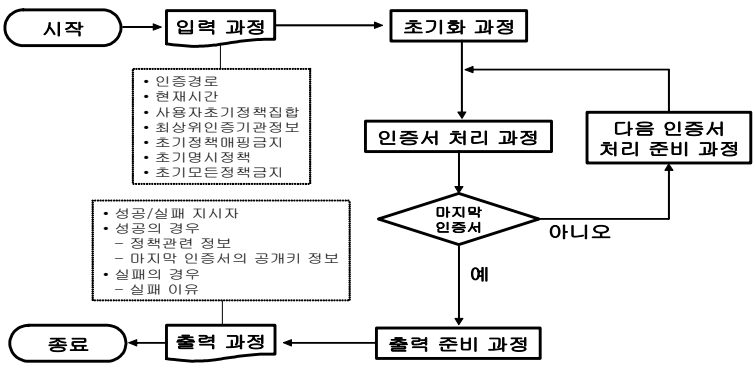
o PrintableString 타입으로 인코딩된 속성 값은 선행 공백문자([스페이스], [탭]) 및 후행 공백문자를 제거하고, 하나 이상의 내부 공백문자는 하나의 [스페이스] 공백문자로 변환 후 비교한다. (예: "Marinanne[스페이스][스페이스]Swanson"은 "Marinanne [스페이스]Swanson"로 변환 됨)

최상위인증기관정보의 유효기간이 현재시각을 포함하고 있는지 검증해야 한다.

## 7. 인증 경로검증 알고리즘

### 7.1 인증서 경로 기본검증

인증서 경로검증 과정은 [그림 1]의 인증서 경로검증 흐름도를 준용해야 한다.




[그림 1] 인증서 경로검증 흐름도

#### 7.1.1 입력 과정

인증서 경로검증 알고리즘을 수행하기 위해 필요한 입력값은 다음과 같다.

(a) 길이 n의 인증경로

신뢰당사자는 n번째 인증서를 검증하기 위해 생성한 인증경로({1, ... , n})는

다음을 만족해야 한다.

- {1, ... , n-1} 중 인증서 x의 소유자는 인증서 x+1의 발급자이어야 한다.
- 인증서 1은 신뢰당사자가 신뢰하는 최상위인증기관정보를 이용해 발급된 인증서이다.
- 인증서 n은 신뢰당사자가 검증하길 원하는 대상인증서이다.

(b) 현재시각(T)

대상인증서의 검증시각을 설정한다. 초기값은 현재시각을 설정해야 한다.

(c) 사용자초기정책집합(user-initial-policy-set)

신뢰당사자가 수용가능한 인증서정책식별자를 설정한다. 초기값은 상호연동 인증서 정책을 포함해야 한다.

(d) 최상위인증기관정보

인증서 경로검증 시 신뢰당사자가 이용하는 신뢰된 정보로써 다음과 같은 정보를 포함하며, 초기값은 '6.인증 경로구축'을 통해 구축된 최상위인증기관 정보를 설정해야 한다.

- 최상위인증기관명칭
- 최상위인증기관공개키알고리즘
- 최상위인증기관공개키
- 최상위인증기관공개키파라미터(선택사항)

(e) 초기정책매핑금지(initial-policy-mapping-inhibit)

인증서 경로검증 절차에서 정책매핑의 수행여부를 설정한다. 초기값은 FALSE로 설정해야 한다.

(f) 초기명시정책(initial-explicit-policy)

사용자초기정책집합(user-initial-policy-set) 중 적어도 하나의 정책이 유효한 정책트리(valid-policy-tree)에 반영되는지를 설정한다. 초기값은 TRUE로 설정해야 한다.

(g) 초기모든정책금지(initial-any-policy-inhibit)

인증서에 포함된 인증서 정책 확장필드 내에 포함된 any-policy를 나타내는 OID의 처리여부를 설정한다. 초기값은 FALSE로 설정해야 한다.

### 7.1.2 초기화 과정

신뢰당사자의 입력값을 기본으로 다음의 상태변수들을 초기화한다.

(a) 유효한정책트리(valid_policy_tree)

인증서 경로검증 과정에서 생성되는 인증서들의 정책연결 정보를 표현한다. 유효한정책트리(valid-policy-tree)의 깊이는 현재 처리된 인증경로의 길이와 같아야 한다. 만약, 어떤 단계에서 유효한 정책이 존재하지 않으면 유효한정책트리(valid-policy-tree)는 NULL로 설정되고, 한번 NULL로 설정되면 더 이상의 인증서 정책은 처리되지 않는다. 유효한정책트리(valid-policy-tree) 안의 각각의 노드는 다음과 같은 요소로 구성되어야 한다.

- valid_policy
- qualifier_set
- criticality_indicator
- expected_policy_set

유효한정책트리(valid_policy_tree)의 초기노드는 다음과 같고, 이 노드의 깊이는 0이다.

- valid_policy : any-policy
- qualifier_set : empty
- criticality_indicator : FALSE
- expected_policy_set : any-policy

(b) 명칭제한관련 변수

(1) 허가된명칭범위(permitted_subtrees)

인증경로 내의 후속 인증서의 소유자 DN과 SAN 확장필드의 값이 속해야 하는 명칭의 범위를 정의하며, 각각의 명칭형태에 따라 허가되는 범위를 가진다. 각각의 명칭형태에 대해서 초기값은 “unbounded”로 설정되며, Name Constraints 확장필드의 permittedSubtrees 필드를 포함한 인증서에 의해 각 명칭형태별로 재설정될 수 있어야 한다.

(2) 배제된명칭범위(excluded_subtrees)

인증경로 내의 후속 인증서의 소유자 DN과 SAN 확장필드의 값이 속하지 않아야 하는 명칭의 범위를 정의하며, 각각의 명칭형태에 따라 배제되는 범위를 가진다. 각각의 명칭형태에 대해서 초기값은 “empty"로 설정되며, Name Constraints 확장필드의 excludedSubtrees 필드를 포함한 인증서에 의해 각 명칭형태별로 재설정 될 수 있어야 한다.

[표 1]은 이용되어야할 명칭형태 및 그 초기값을 나타낸다.

[표 1] 명칭형태

| 명칭형태 | 허가된명칭범위 (permitted_subtrees)의 초기값 | 배제된명칭범위 (excluded_subtrees)의 초기값 |
|---|---|---|
| rfc822Name | unbounded | empty |
| dNSName | unbounded | empty |
| directoryName | unbounded | empty |

(c) 정책관련 변수

정책관련 변수는 다음과 같다.

(1) 명시정책(explicit_policy)

NULL이 아닌 유효한정책집합(valid_policy_tree)의 존재 여부를 표시하는 정수로, 신뢰당사자에 의해 초기명시정책(initial-explicit-policy)이 설정되었다면 초기값은 0으로, 그렇지 않으면 n+1로 초기화된다. 인증서의 Policy Constraints 확장필드의 requireExplicitPolicy 필드를 포함한 인증서에 의해 이 값은 재설정 될 수 있어야 한다.

(2) 모든정책금지(inhibit_any-policy)

any-policy를 나타내는 OID의 처리여부를 표시하는 정수로 모든정책금지(inhibit_any-policy)가 0일 경우, CP 확장필드 안에 포함된 any-policy는 유효한정책트리(valid-policy-tree)에 포함되지 않는다.

신뢰당사자에 의해 초기모든정책금지(initial-any-policy-inhibit)가 설정되었다면, 초기값은 0으로, 그렇지 않으면 n+1로 초기화된다. 인증서의 Inhibit Any-Policy 확장필드 내의 inhibitAnyPolicy 필드를 포함한 인증서에 의해 이 변수는 재설정 될 수 있다.

(3) 정책매핑(policy_mapping)

인증서 정책의 매핑여부를 표시하는 정수로 정책매핑(policy_mapping)이 0일 경우, 처리되는 인증서가 Policy Mapping 확장필드를 가지고 있더라도 정책매핑은 수행되지 않는다.

신뢰당사자에 의해 초기정책매핑금지(initial_policy_mapping_inhibit)가 설정되었다면, 초기값은 0으로, 그렇지 않으면 n+1로 초기화된다. 인증서의

Policy Constraints 확장필드 내의 inhibitPolicyMapping 필드를 포함한 인증서에 의해 이 변수는 재설정 될 수 있어야 한다.

(d) 인증경로최대허용길이(max_path_length)

인증경로를 구성하는 인증서 수를 제한하는 정수로 초기값은 n이 되며, 인증서의 Basic Constraints 확장필드 내에 pathLenConstraint 필드를 포함한 인증서에 의해 이 변수는 재설정 될 수 있어야 한다.

(e) 임시변수

(1) 임시공개키알고리즘(working_public_key_algorithm)

i번째 인증서의 서명을 검증하기 위해 필요한 i-1 인증서의 공개키 알고리즘을 나타내며, 최상위인증기관공개키알고리즘으로 초기화된다.

(2) 임시공개키(working_public_key)

i번째 인증서의 서명을 검증하기 위해 필요한 i-1 인증서의 공개키를 나타내며, 최상위인증기관공개키로 초기화된다.

(3) 임시공개키파라미터(working_public_key_parameters)

i번째 인증서의 서명을 검증하기 위해 필요한 i-1 인증서의 공개키와 관련된 파라미터를 나타내며, 최상위인증기관공개키파라미터로 초기화된다.

(4) 임시발급자 식별명칭(working_issuer_name)

i번째 인증서의 명칭 연결을 검증하기 위해 필요한 i-1인증서의 소유자 DN을 나타내며, 최상위인증기관명칭으로 초기화된다.

### 7.1.3 인증서 처리 과정

인증경로에 포함된 모든 인증서에 대해 다음의 과정을 수행한다.

(a) 기본 검증을 수행한다. 단, 이 과정은 인증서 경로구축 과정에서 수행될 수 있다.

(1) 임시공개키, 임시공개키파라미터, 임시공개키알고리즘을 이용해 인증서 i의 서명을 검증하여야 한다. 만약, 인증서 i가 인증경로의 첫 번째 인증서라면 임시변수들은 최상위인증기관정보이다. 그렇지 않다면, 임시변수들은 i-1 인증서의 정보이다.

(2) 인증서 유효기간이 현재시각(T)을 포함하는지 검증한다.

(3) 인증서가 현재시각(T)에 폐지 및 효력정지 되지 않았음을 검증하여야 한다. 인증서의 상태를 검증하기 위해 CRL을 이용할 수 있고, 또는 [KCAC.TS.OCSP]에서 정의하고 있는 실시간 인증서 상태확인 기술을 준용할 수 있다.

(4) 인증서의 발급자 DN이 임시발급자 식별명칭과 같은지 검증한다. 만약, 인증서 i가 인증경로의 첫 번째 인증서라면 임시발급자명칭은 최상위인증기관 명칭이다. 그렇지 않다면, 임시발급자명칭은 i-1 인증서의 소유자 명칭이다.

(b) 허가된명칭범위(permitted_subtree) 검증

인증서 i가 자가발행 인증서이고 인증경로의 마지막 인증서가 아니라면, 이 과정은 수행되지 않는다. 그렇지 않다면, 인증서의 소유자 DN이 허가된명칭범위(permitted-subtrees)의 directoryName 명칭형태의 범위에 포함되는지 검증한다.

또한, 인증서에 SAN 확장필드가 존재한다면, 이 확장필드가 포함하고 있는 값들이 허가된명칭범위(permitted-subtrees)가 가지고 있는 각 명칭형태의 범위에 포함되는지 검증한다.

(c) 배제된명칭범위(excluded_subtree) 검증

인증서 i가 자가발행 인증서이고 인증경로의 마지막 인증서가 아니라면, 이 과정은 수행되지 않는다. 그렇지 않다면, 인증서의 소유자 DN이 배제된명칭범위(excluded-subtrees)의 directoryName 명칭형태의 범위에 포함되지 않는지 검증한다.

또한, 인증서에 SAN 확장필드가 존재한다면, 이 확장필드가 포함하고 있는 값들이 허가된명칭범위(permitted-subtrees)가 가지고 있는 각 명칭형태의 범위에 포함되지 않는지 검증한다.

(d) 유효한정책트리(valid_policy_tree)를 처리한다.

(1) 인증서에 CP 확장필드가 존재하고 유효한정책트리(valid_ policy_tree)가 NULL이 아닐 때, 인증서 안의 각 인증서 정책에 대해 유효한정책트리(valid_policy_tree)를 처리한다.

1) 인증서 i의 인증서 정책 P가 any-policy가 아니고, 유효한정책트리(valid_policy_tree) 내 i-1 깊이 노드들 중에서 expected_policy_set이 인증서 정책 P를 포함하는 노드들가 있을 경우, 인증서 정책 P에 해당하는 노드를

하부에 생성하고 유효한정책트리(valid_policy_tree)를 아래와 같이 설정한다.
(P-OID : 인증서 i의 인증서 정책 OID, P-Q : 정책 P의 qualifier_set)

- valid_policy : P-OID
- qualifier_set : P-Q
- criticality_indicator : uninitialized
- expected_policy_set : P-OID

2) 인증서 i의 인증서 정책 P가 any-policy가 아니고 1)이 수행되지 않았다면, 유효한정책트리(valid_policy_tree) 내 i-1 깊이의 노드들 중에서, expected_policy_set이 any-policy인 노드들에 대해서 정책 P에 해당하는 노드를 다음과 같이 하부에 생성한다.
(P-OID : 인증서 i의 인증서 정책 OID, P-Q : 정책 P의 qualifier_set)

- valid_policy : P-OID
- qualifier_set : P-Q
- criticality_indicator : uninitialized
- expected_policy_set : P-OID

3) 인증서 i의 인증서 정책 P가 any-policy이면, 유효한정책트리(valid_policy_tree) 내 i-1 깊이의 노드들 중에서 expected_policy_set이 포함하는 모든 노드에 대해서 다음과 같은 하부 노드를 생성한다.
(AP-Q : 인증서 i의 qualifier_set)

- valid_policy : i-1 노드의 expected_policy_set에 해당하는 정책 OID 중 하나
- qualifier_set : AP-Q
- criticality_indicator : uninitialized
- expected_policy_set : 이 노드의 valid_policy 값과 동일

단, 이 과정은 모든정책금지(inhibit_any-policy)가 0보다 크거나 또는 인증경로의 마지막이 아닌 자가발행 인증서일 경우에 수행되어야 한다.

4) 인증서 i의 인증서 정책 P가 any-policy이고, 유효한정책트리(valid_policy_tree) 내 i-1 깊이의 노드들 중에서 expected_policy_set이 any-policy를 포함하는 노드들에 대하여, 다음과 같은 하부 노드를 생성한다.
(AP-Q : 인증서 i의 qualifier_set)

- valid_policy : any-policy
- qualifier_set : AP-Q

- criticality_indicator : uninitialized
- expected_policy_set : any-policy

단, 이 과정은 모든정책금지(inhibit_any-policy)가 0보다 크거나 또는 인증경로의 마지막이 아닌 자가발행 인증서일 경우에 수행된다.

(2) 유효한정책트리(valid_policy_tree) 내 i-1 또는 그보다 깊이가 작은 노드들 중 하부 노드를 가지지 않으면, 그 노드를 삭제한다. 이 조건을 만족하는 노드가 없을 때까지 이 과정을 반복 수행한다.

(3) 인증서의 CP 확장필드가 Critical이면 i 깊이에 해당되는 모든 노드들의 criticality_indicator를 TRUE로 설정하고, Critical이 아니면 FALSE로 설정한다.

(e) CP 확장필드가 인증서 내에 없다면, 유효한정책트리(valid_policy_tree)는 NULL로 설정한다. 한번 NULL로 유효한정책트리(valid_policy_tree)가 설정되면 그 값은 변하지 않는다.

(f) 명시정책(explicit_policy)이 0보다 크거나 또는 유효한정책트리(valid_policy_tree)가 NULL이 아닌지 검증한다. 명시적정책(explicit_policy)이 0이고, 유효한정책트리(valid_policy_tree)가 NULL일 경우는 검증에 실패한다.

처리되는 인증서가 인증경로의 마지막 인증서라면 '7.1.5. 출력 준비 과정'을 수행하고, 처리되는 인증서가 마지막 인증서가 아니라면 '7.1.4. 다음 인증서 처리 준비 과정'을 수행한다.

### 7.1.4 다음 인증서 처리 준비 과정

다음 인증서 경로처리를 준비하기 위해 다음의 과정을 수행한다.

(a) 인증서 정책매핑

(1) 인증서 내에 Policy Mapping 확장필드가 존재한다면, 이 확장필드 내의 issuerDomainPolicy 필드와 subjectDomainPolicy 필드에 any-policy이 존재하지 않는지 검증한다.

(2) 인증서 내에 Policy Mapping 확장필드가 존재할 경우 다음을 수행한다.

1) 정책매핑(policy_mapping)필드가 0보다 크고 유효한정책트리(valid_policy_tree) 내 i 깊이의 노드들 중에서 valid_policy가 issuerDomainPolicy와 일치하는

노드들에 대해서, i 노드의 expected_policy_set을 subjectDomainPolicy 필드의 값으로 설정한다.

(issuerDomainPolicy : A-OID, subjectDomainPolicy : B-OID)

- valid_policy : A-OID
- qualifier_set : 인증서 i의 qualifier_set
- criticality_indicator : 인증서 i의 criticality
- expected_policy_set : B-OID

2) 유효한정책트리(valid_policy_tree) 내 i 깊이의 노드들 중에서 valid_policy가 issuerDomainPolicy와 일치하지 않고 any-policy를 가지는 노드가 있을 경우, 그 상위 노드에 하부 노드를 생성하고, 하부 노드를 다음과 같이 설정한다.

(issuerDomainPolicy : A-OID, subjectDomainPolicy : B-OID)

- valid_policy : A-OID
- qualifier_set : 인증서 i의 qualifier
- criticality_indicator : 인증서 i의 criticality
- expected_policy_set : B-OID

3) 정책매핑(policy_mapping)이 0이면, 깊이 i의 유효한정책트리(valid_policy_tree)에서 valid_policy가 issuerDomainPolicy와 같은 노드들을 삭제한다.

(3) 유효한정책트리(valid_policy_tree)의 i-1 또는 그보다 깊이가 작은 노드들 중 하부 노드를 가지지 않으면, 그 노드를 삭제한다. 이 조건을 만족하는 노드가 없을 때까지 이 과정을 반복 수행한다.

(b) i+1 인증서를 검증하기 위해 임시변수들을 재설정한다.

(1) 임시발급자 식별명칭(working_issuer_name)을 i번째 인증서의 소유자 DN으로 재설정한다.

(2) 임시공개키(working_public_key)를 현재 처리되는 i번째 인증서의 공개키로 재설정한다.

(3) 인증서의 SKI 필드 내의 algorithm 필드 값이 NULL이 아닌 파라미터를 가지고 있다면, 임시공개키파라미터(working_public_key_parameters)를 이 파라미터로 재설정한다. 인증서의 SKI 확장필드 내의 algorithm 필드 값이 NULL인 파라미터를 가지거나 또는 파라미터가 빠져있을 경우, SKI 확장필드 내의 algorithm 필드와 임시공개키알고리즘(working_public_key_algorithm)를

비교한다. 만약, 두 값이 서로 다르다면 임시공개키파라메터(working_public_key_parameters)를 NULL로 설정하고, 두 값이 서로 같다면, 임시공개키파라메터(working_ public_key_parameters)를 변경하지 않는다.

(4) 임시공개키알고리즘(working_public_key_algorithm)을 인증서의 SKI 필드 내의 algorithm 필드 값으로 재설정한다.

(c) 명칭 제한 관련 변수들을 재설정한다. 인증서에 Name Constraints 확장필드가 존재한다면, 허가된명칭범위(permitted_subtrees)와 배제된명칭범위(excluded_subtrees)를 재설정한다.

(1) 인증서에 permittedSubtrees 필드가 존재한다면, 각각의 명칭형태에 따라 허가된명칭범위(permitted_subtrees)를 허가된명칭범위(permitted_subtrees)와 PermittedSubtree의 교집합으로 재설정한다.

(2) 인증서에 excludedSubtrees 필드가 존재한다면, 각각의 명칭형태에 따라 배제된명칭범위(excluded_subtrees)를 배제된명칭범위(excluded_subtrees)와 ExcludedSubtree의 합집합으로 재설정한다.

(d) 현재 처리되는 인증서가 자가발행 인증서가 아니라면, 정책관련 상태변수들을 재설정한다.

(1) 명시정책(explicit_policy)이 0이 아니면, 이 값을 1 감소한다.

(2) 정책매핑(policy-mapping)이 0이 아니면, 이 값을 1 감소한다.

(3) 모든정책매핑(inhibit_any-policy)이 0이 아니면, 이 값을 1 감소한다.

(4) 인증서의 Policy Constraints 확장필드 내에 requireExplicitPolicy 필드가 존재하고 이 값이 명시정책(explicit_policy)보다 작다면, 명시정책(explicit_policy)을 requireExplicitPolicy 필드의 값으로 재설정한다.

(5) 인증서의 Policy Constraints 확장필드 내에 inhibitPolicyMapping 필드가 존재하고 이 값이 정책매핑(policy_mapping)보다 작다면, 정책매핑(policy_mapping)을 inhibitPolicyMapping 필드의 값으로 재설정한다.

(6) 인증서의 Inhibit Any-Policy 확장필드 내에 inhibit_any-policy 필드가 존재하고 이 값이 모든정책금지(inhibit_any-policy)보다 작다면, 모든정책금지(inhibit_any-policy)를 inhibitAnyPolicy 필드의 값으로 재설정한다.

(e) 인증서의 Basic Constraints 확장필드 내에 cA 필드의 값을 이용해 인증서 i가 인증기관 인증서인지 검증한다.

(f) 인증서가 자가발행되지 않았다면, 인증경로최대허용길이(max_path_length)가 0 보다 큰지 검사하고 이 값을 1 감소한다. 그리고, 인증서의 Basic Constraints 확장필드 내에 pathLengthConstraint 필드가 존재하고 이 값이 인증경로최대허용길이(max_path_length)보다 작다면, 인증경로최대허용길이(max_path_length)를 pathLengthConstraint 필드의 값으로 재설정한다.

(g) 인증서의 Key Usage 확장필드 내에 keyCertSign 비트가 설정되어 있는지 검증한다.

(h) 기타 critical 확장필드가 존재할 경우, 해당 필드는 반드시 처리해야 하며, 인지된 non-critical 확장필드일 경우에도 처리해야 한다.

7.1.5 출력 준비 과정

(a) 자가발행 인증서가 아니고, 명시정책(explicit_policy)이 0이 아니면, 명시정책(explicit_policy)을 1 감소한다.

인증서의 Policy Constraints 확장필드 내에 requireExplicitPolicy 필드가 존재하고 이 값이 명시정책(explicit_policy)보다 작다면, 명시정책(explicit_policy)을 requireExplicitPolicy 필드의 값으로 재설정한다.

(b) 출력을 위해 임시변수들을 재설정한다.

(1) 임시공개키(working_public_key)를 현재 처리되는 i번째 인증서의 공개키로 재설정한다.

(2) 인증서의 SKI 확장필드 내의 algorithm 필드 값이 NULL이 아닌 파라미터를 가지고 있다면, 임시공개키파라미터(working_ public_key_parameters)를 이 파라미터로 재설정한다.

인증서의 SKI 확장필드 내의 algorithm 필드 값이 NULL인 파라미터를 가지거나 또는 파라미터가 빠져있을 경우, SKI 확장필드 내의 algorithm 필드와 임시공개키알고리즘(working_ public_key_algorithm)를 비교한다. 만약, 서로 다르다면, 임시공개키파라메터(working_public_key_parameters)를 NULL로 설정한다.

(3) 임시공개키알고리즘(working_public_key_algorithm)을 인증서의 SKI 확장필드 내의 algorithm 필드 값으로 재설정한다.

(c) 기타 critical 확장필드가 존재할 경우에는 꼭 처리하여야 하며, 인지된 non-critical 확장필드일 경우에도 처리해야 한다.

(d) 사용자초기정책집합(user-initial-policy-set)과 유효한정책트리(valid_policy_tree)의 교집합을 계산한다.

(1) 유효한정책트리(valid_policy_tree)가 NULL이면, 유효한정책트리(valid_policy_tree)와 사용자초기정책집합(user-initial-policy-set)의 교집합은 NULL이다.

(2) 유효한정책트리(valid_policy_tree)가 NULL이 아니고, 사용자초기정책집합(user-initial-policy-set)이 any-policy이라면, 교집합의 결과는 유효한정책트리(valid_policy_tree)이다.

(3) 유효한정책트리(valid_policy_tree)가 NULL이 아니고, 사용자초기정책집합(user-initial-policy-set)이 any-policy가 아니라면, 교집합은 다음과 같이 계산된다.

1) valid_policy_node_set을 설정한다. valid_policy_node_set은 부모노드의 valid_policy가 any-policy인 노드들의 집합이다.

2) 만약, valid_policy_node_set의 노드 중 사용자초기정책집합(user-initial-policy-set)에 없고 any-policy가 아닌 노드와 그 하부노드들을 유효한정책트리(valid_policy_tree)에서 삭제한다.

3) 만약, 유효한정책트리(valid_policy_tree) 내 n 깊이에 any-policy를 가지는 노드가 존재하고 사용자초기정책집합(user-initial-policy-set)이 any-policy가 아니라면, 다음과 같이 실행된다.

a. n 깊이의 any-policy를 valid_policy로 갖는 노드의 qualifier_set을 P-Q로 설정한다.

b. valid_policy_node_set에 포함되지 않는 사용자초기정책집합(user-initial-policy-set)안의 정책 P들에 대해 n-1 깊이에서 any-policy를 가지는 노드의 하부에 다음과 같은 노드를 생성한다.
(P-OID : 정책 P의 OID)
・valid_policy : P-OID

· qualifier_set : P-Q
· criticality_indicator : 깊이 n의 criticality
· expected_policy_set : P-OID

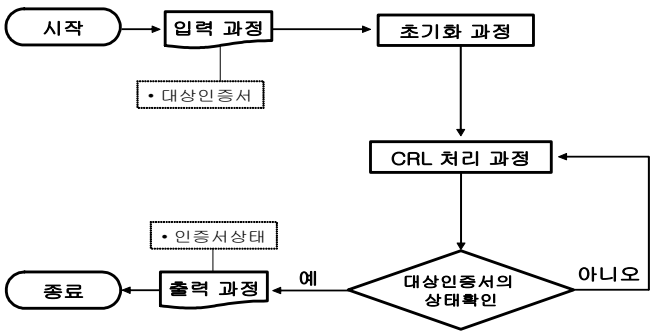
c. any-policy를 가지는 깊이 n의 노드를 삭제한다.

4) 유효한정책트리(valid_policy_tree)의 i-1 또는 그보다 깊이가 작은 노드들 중 하부 노드를 가지지 않으면, 그 노드를 삭제한다. 이 조건을 만족하는 노드가 없을 때까지 이 과정을 반복 수행한다.

(e) 명시정책(explicit_policy)이 0보다 크거나 또는 유효한정책트리(valid_policy_tree)가 NULL이 아닌지 검증한다.

## 7.2 CRL 검증 알고리즘

인증서의 상태를 검증하기 위해 CRL을 이용할 경우, [그림 2] CRL 검증 알고리즘의 흐름도를 준용해야 한다.




[그림 2] CRL 검증 알고리즘 흐름도

### 7.2.1 입력 과정

인증서의 상태검증을 위해 다음의 값들을 입력한다.

(a) 대상인증서

신뢰당사자가 상태정보를 확인하고자 하는 인증서로써, 대상인증서의 정보를 이용해 신뢰당사자는 상태정보를 확인할 수 있다.

7.2.2 초기화 과정

(a) 인증서상태(cert_status)

이 변수는 인증서의 상태를 나타내고 다음의 값들을 가질 수 있으며, “UNREVOKED"으로 초기화되어야 한다.

7.2.3 CRL 처리 과정

(a) 인증서를 검증하기 위해 CRL을 획득한다.

(1) CRL 경로를 구축하기 위해, 신뢰당사자는 대상인증서의 AKI 확장필드 내에 포함된 KeyIdentifier와 authorityCertIssuer 및 authority CertSerialNumber가 대상인증서의 상태 검증을 위해 이용되는 CRL의 AKI 확장필드 내에 포함된 KeyIdentifier와 authorityCertIssuer 및 authorityCertSerialNumber와 서로 일치하는지를 검증한다.

그러나 만약 대상인증서에 대한 CRL이 간접 CRL 인 경우, 대상인증서의 CRL 분배점 확장필드에 DistributionPoint 필드 내 cRLIssuer 필드와 CRL의 발급자 DN 값이 같은지 검사한다. 또한, CRL의 IDP 확장필드에 IndirectCRL 필드가 설정되었는지를 검증하여 CRL을 획득한다.

(2) 현재시각이 신뢰당사자가 소유하고 있는 CRL의 NextUpdate보다 이후 일 때 새로운 CRL을 획득하여, 새로운 CRL의 NextUpdate가 현재시각 이후인지 검증한다.

(b) CRL의 발급자 DN과 범위를 검증한다.

(1) 대상인증서의 발급자 DN이 CRL의 발급자 DN과 일치하는지 검사한다. 인증서의 CRLDP 확장필드의 DistributionPoint 필드 내에 cRLIssuer 필드가 존재하는 경우, 이를 수행하지 않는다.

(2) CRL이 IDP 확장필드를 포함하고 있다면, 다음을 검증한다.

1) IDP 확장필드 내의 DistributionPointName 필드와 인증서의 CRLDP 확장필드 내의 DistributionPointName 필드가 존재한다면, IDP 확장필드의 DistributionPointName 필드 중 하나는 인증서의 CRLDP 확장

필드 내 DistributionPointName 중 하나와 일치해야 한다.

2) 만약, IDP 확장필드 내에 DistributionPointName 필드가 존재하고 대상 인증서의 CRLDP 확장필드 내에 DistributionPointName 필드가 존재하지 않을 경우, CRL의 IDP 확장필드 내에 DistributionPointName 필드 중 하나는 인증서의 CRLDP 확장필드 내 cRLIssuer 필드와 일치해야 한다.

(c) CRL을 검증하기 위해 CRL 발급자에 대한 인증경로를 생성하고 검증한다. 만약, CRL 발급기관의 인증서에 Key Usage 확장필드가 존재한다면 cRLSign로 설정되었음을 검증한다.

(d) CRL의 서명을 검증한다.

(e) CRL에서 상태를 확인하고자 하는 대상 인증서의 일련번호가 존재하는지 검증한다. 그리고 만약, 대상인증서의 CRLDP 확장필드 내 DistributionPoint 필드에 cRLIssuer 필드가 존재하면, 대상 인증서의 발급자 DN과 CRL의 Revoked Certificates 필드 내 CRL 엔트리 확장필드에 있는 certificateIssuer 필드가 서로 일치하는지 검증한다.

(f) 만약, 일치하는 개체가 존재하면 인증서상태(cert_status)에 CRL 엔트리 확장필드의 reasoncode 필드의 값을 설정한다. 일치하는 개체가 존재하지 않으면, 인증서상태(cert_status)를 UNREVOKED로 설정한다.

### 7.2.4 출력 과정

대상 인증서의 인증서 상태(cert-status)를 출력한다.

부록 1. 규격 연혁

| 버전 | 제・개정일 | 제・개정내역 |
|---|---|---|
| v1.00 | 2004년 6월 | ・"공인인증서 경로검증 기술규격"으로 제정 |
| v1.10 | 2008년 10월 | ・관련 국내 표준 및 규격 갱신 내용 반영<br>・법률 공포번호가 해당 법률 개정시마다 변경되는 점을 고려하여 법령명으로 개정 |
| v1.11 | 2009년 9월 | ・공인전자서명인증체계 기술규격 개정에 따라 본문 내용 중 관련 기술규격 참조 변경 사항 개정 |