通信情報保護學會誌
第8卷 第1號, 1998. 3

디렉토리 서비스에 관한 고찰
-제 2 부 : 분산된 환경에서의 DSA의 동작과 디렉토리 프로토콜-
(X.518과 X.519)

정 윤 정*, 김 준 태*, 오 수 현*, 정 병 천*, 원 동 호*

요 약

정보통신기술의 발달과 인터넷의 이용확대로 물리적인 현실세계에서 이루어지는 것들이 가상현실로 옮겨져 가고 있다. 전자 상거래도 이에 빠른 속도로 발전하고 있고, 선진국에서는 이미 국가적 차원에서 추진 중이다. 우리나라에서도 정보통신부가 전자상거래를 위한 기술과 더불어 법/제도 개선을 추진 중이다. 전자상거래의 정보보호를 위하여 필수적인 요소는 전자서명을 위한 전자인증제도이다. 전자서명을 위해서 공개키 기반구조기술이 요구된다. 이러한 공개키 기반구조는 디렉토리 서비스를 통해 이루어진다.

1. 서 론

컴퓨터의 보급 확대와 통신기술의 발전으로 일부에서는 일상업무가 현실 세계가 아닌 가상 세계에서 전자적으로 이루어지고 있다. 선진국에서는 이러한 가상공간의 대두로 인해 전자상거래를 국가경쟁 사업으로 추진중이다. 미 국 은 NII(National Information Infrastructure)나 GII(Global Information Infrastructure)를 통해 세계를 하나의 공간으로 간주하고 전자상거래 등의 전자적인 사업들의 기반기술을 갖추어 나가고 있다. 특히 이 사업은 정보보호 분야에서도 중요한 의미를 갖는다. 이것은 가상공간을 논리적인 하나의 공간으로 보고 네트워크를 구축하고, 또한 전자서명을 위한 전자인증제도가 마련중이다. 전자인증제도가 실현되기 위해서는 공개키 기반구조가 구축되어야 한다. 공개키 기반구조는 세계를 논리적인 공간을 나누어 운용·관리를 한다. 이러한 논리적인 공간을 디렉토리라 하고, 디렉토리 서비스는 실세계에서 일련의 정보객체들을 논리적 데이터 베이스를 유지하기 위한 개방 시스템의 집합이다. 디렉토리 사용자는 디렉토리에 액세스함으로써 디렉토리 서비스를 받는다. 즉 디렉토리 사용자 에이전트는 실제로 디렉토리에 액세스 하고, 특정 사용자를 위한 서비스를 받기 위해서 디렉토리와 상호작용을 한다. 디렉토리는 하나 또는 그 이상의 액세스 점을 제공하는데 이 점에서 이러한 액세스가 이루어진다. ITU-T(International Telecommunication Union) 권고 X.500 시리즈에서 X.500은 디렉토리의 개념과 모델 및 서

* 성균관대학교 정보공학과

비스를 설명한다. X.501은 기능적/관리적 모형을 기능적으로 또 행정적으로 디렉토리를 분산시킬 수 있는 방법을 정의한다. X.509는 디렉토리에 저장되는 인증정보의 형태를 규정하고 인증정보를 디렉토리에서 얻는 방법에 대해 설명하고 인증정보가 형성되고 디렉토리에 저장되는 방법에 대한 가정을 기술한다. X.511은 디렉토리에 의하여 제공된 외부적으로 파악되는 서비스를 추상적 방법으로 정의한다. X.518은 분산된 디렉토리 응용에 참여하는 DSA의 동작을 규정한다. 이 동작은 DIB가 많은 DSA를 통하여 광범위하게 분산된 환경하에서 일관성있는 서비스를 보장하기 위해 설계된 것이다. X.519는 추상서비스를 이행하는 디렉토리 액세스 프로토콜, 디렉토리 시스템 프로토콜, 디렉토리 정보 섀도 프로토콜, 디렉토리 운용 결합 관리 프로토콜을 설명한다. X.520은 디렉토리의 모든 적용 분야의 유용한 속성과 규칙에 대해 정의한다. X.521은 디렉토리의 응용 범위에 걸쳐서 유용할 수도 있는 객체 부류와 명칭 형식을 규정한다. X.525는 디렉토리 시스템 에이전트가 정보의 복사에 대한 운용과 관리를 설명한다.

본 논문에서는 X.518과 X.519의 내용을 자세히 알아본다.

2. 분산된 디렉토리 운용에서의 DSA 동작

X.518는 분산된 디렉토리 운용에 참여하는 DSA의 동작을 규정하고, DIB가 많은 DSA를 통하여 광범위하게 분산된 환경하에서 일관성 있는 서비스를 보장하기 위해서 설계되었다. 추상적 디렉토리 대상을 재정의하고 이 재정의는 분산 디렉토리 서비스를 집합적으로 구성하는 하나 또는 그 이상의 DSA 대상의 집합으로 표현된다. 또한 DIB가 하나 또는 그 이상의 DSA에 분산될 수 있는 방법을 설명한다. DIB가 두 개 이상의 DSA에 분산되는 경우에 DIB 전체가 구성 엔트리를 갖고 있는 모든 DSA에서 액세스할 수 있다는 것을 보장하는 지식이 있다. 일반적으로 디렉토리는 분산되어 있으므로 디렉토리 조회는 연쇄 또는 리퍼럴할 수 있는 DSA에 의해서 이행될 것이고, 요구에 응답하는 DSA는 적절한 절차를 통해서 이루어진다.

2.1 정보 유형

DSA 추상적 서비스의 다양한 동작을 정의하는데 많은 정보유형을 사용한다.

2.1.1 연쇄 인수

연쇄인수는 요구되는 정보를 DSA에 전달하기 위한 각각의 연쇄된 동작이다.

각 요소는 다음과 같은 의미를 갖는다.

nameResolveOnMAster	[16]	BOOLEAN DEFAULT FALSE
excludeShadows	[15]	BOOLEAN DEFUALT FALSE
exculsions	[14]	Exclusions OPTIONAL
authenticationLevel	[13]	AuthenticaiotnLevel OPTIONAL

uniqueIdntifier	[12]	UniaueIdentifier OPTIONAL
entryOnly	[11]	BOOLEAN DEFAULT FALSE
securityParameters	[10]	SecurityParameters DEFAULT{}
timeLimit	[9]	UTCTime Opntional
info	[8]	DomainInfo OPTIONAL
referenceType	[7]	ReferenceType DEFAULT superior
returnCrossRefs	[6]	BOOLEAN DEFAULT FALSE
aliasRDNs	[5]	INTEGER DEFAULT FALSE
aliasDereferenced	[4]	BOOLEAN DEFAULT FALSE -- abstract unless aliasDereferenced is TRUE
TraceInformation	[3]	TraceInformation
OperationProgress	[2]	OperationProgress DEFAULT{nameResolutionPhase notStarted}
targetObject	[1]	DistinguishedName OPTIONAL
originator	[0]	DistinguishedName OPTIONAL

〈그림 1〉 ChainingArguments의 자료구조

2.1.2 연쇄 결과

연쇄 결과는 각각의 동작의 결과에 존재하며 동작을 지도한 DSA에 피드백을 제공한다.

이것은 동작의 전부 또는 일부의 이행이 서로 다른 DSA 또는 DSA들에서 어떻게 계속될 수 있는지를 기술한다. 관련 DSA가 요구 그 자체를 전파할 수 없을 경우 전형적으로 리퍼럴로 응답된다.

alreadySearched	[3]	Exclusions OPTIONAL
SecurityParameters	[2]	SecurityParameters DEFAULT{}
crossReferencess	[1]	SEQUENCE OF CrossReference OPTIONAL
info	[0]	DomainInfo OPTIONAL

〈그림 2〉 ChainingArguments의 자료구조

2.1.3 동작 진행

동작진행은 몇몇의 DSA가 참석해야 하는 동작의 수행에서 진행의 상태를 기술한다.

operationProgress	[2]	OperationProgress
targetObject	[1]	Name OPTIONAL
dsa	[0]	Name

〈그림 3〉 OperationProgress의 자료구조

2.1.4 추적 정보

추적 정보 값은 동작의 수행시 관련되는 DSA의 기록을 앞쪽으로 전달한다. 이 기록은 DIT에서 별명 루프의 불일치한 지식이나 존재에 의해 생기는 루프의 존재를 검출하거나 피하기 위해 이용된다.

TraceInformation ::= SEQUENCE OF TraceItem

nextRDNToBeResolved		[1]	INTECER OPTIONAL
nameResolutionPhase	completed (3)	[0]	ENUMERATED
	proceeding (2)		
	notStarted (1)		

〈그림 4〉 TraceItem의 자료구조

2.1.5 참조유형

참조유형 값은 권고안에 정의된 여러 가지 종류의 참조 중 하나를 표시한다.

self	(8)
ImmediateSupuior	(7)
master	(6)
Supplier	(5)
nonSpecificSubordinate	(4)
cross	(3)
subordinate	(2)
superior	(1)

〈그림 5〉 ReferenceType의 자료구조

2.1.6 액세스 점 정보

액세스점 간은 디렉토리, 구체적으로 DSA에 액세스할 수 있는 특정 지점을 식별한다. 액세스점은 관련된 DSA의 Name과, 그 DSA와의 OSI통신에서 이용될 PresentationAddress를 갖는다.

protocolInformation	[2]	SET OF ProtocolInformation OPTIONAL
address	[1]	PresentationAddress
ae-title	[0]	Name

〈그림 6〉 AccessPoint의 자료구조

2.1.7 Exclusions

연쇄 인수의 exclusion 요소는 목표 대상의 많은 수의 하위종속 엔트리 탐색 동작의 전망을 제한하는데 사용되며 모든 그의 하위종속과 함께 목표 대상은 탐색동작의 과정에서 포함되어서는 안 된다. exclusion요소는 ASN.1유형 exclusion의 값으로 정의된다.

Exclusions ::= SET OF RDNSequence

2.1.8 연속 참조

연속 참조는 동작의 전부 또는 일부의 이행이 서로 다른 DSA 또는 DSA들에서 어떻게 계속될 수 있는지를 기술한다. 관련 DSA가 요구 그 자체를 전파할 수 없거나 전파를 하지 않으려 할 때 전형적으로 리퍼럴로 응답된다.

nameResolveOnMaster	[9]'	BOOLEAN DEFAULT FALSE
returnToDUA	[8]	BOOLEAN DEFAULT FALSE
exclusions	[7]	Exclusion OPTIONAL
entryOnly	[6]	BOOLEAN DEFAULT FALSE
accessPoints	[5]	SET OF AccessPointLnformation
referenceType	[4]	ReferenceType
rdnsResolved	[3]	INTEGER OPTIONAL
operationProgress	[2]	OperationProgress
aliasedRDNs	[1]	INTEGER OPTIONAL
targetObject	[0]	Name

〈그림 7〉 ContinuationReference의 자료구조

2.2 결합과 비결합

DSABind 및 DSAUnbind는 각각 다른 DSA를 액세스하는 기간의 시작과 끝에서 DSA에 의하여 이용된다.

2.2.1 DSA 결합

DSABind 동작은 디렉토리 서비스를 제공하는 두 DSA간 상호작용 기간의 시작에 이용된다.

DSABind ::= BIND
ARGUMENT DirectoryBindResult
RESULT DirectoryBindError
BIND-ERROR

2.2.2 DSA비결합

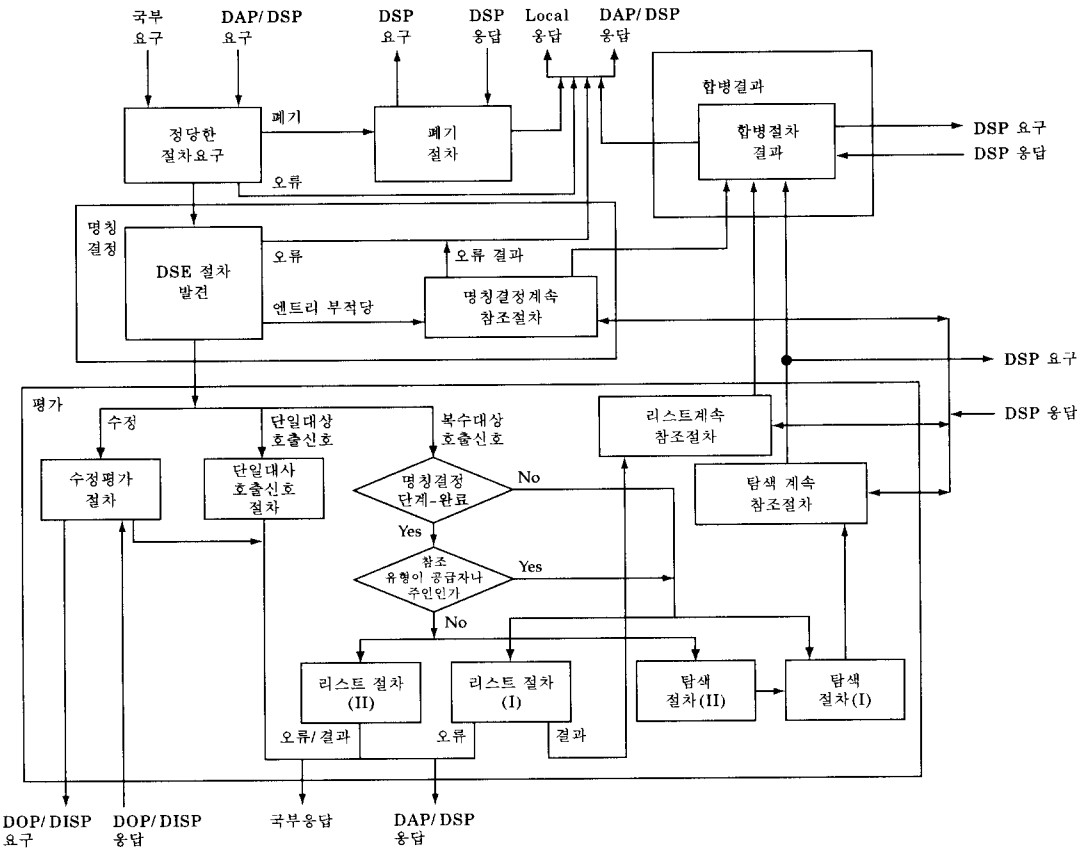
DSAUnbind 디렉토리 서비스를 제공하는 두 DSA들간 상호작용 기간에 이용된다.

DSAUnbind UNBMD ::= UNBIND

여기에서 인수, 결과 또는 오류가 없다.

2.3 동작절차

동작 절차는 인수, 결과 및 오류의 항목으로 인터페이스를 이루고, 다음의 그림에 의하여 설명된다.



〈그림 8〉 X.518 동작절차

각 수신된 요구 즉 DAP/DSP의 요구를 처리하기 위하여 동작 실행자에 의하여 실행되는 절차는 다음 단계에 의하여 정의된다. 별명 역 참조로 인하여 이 절차는 자신을 호출할 수도 있고, 이 경우 국부 대답이 응답된다.

1) 요구 확인 중에 오류를 되면 국부적으로 또는 DAP/DSP를 거쳐 이 오류에 응답한다.

2) 수신된 동작이 포기동작이었으면 포기 절차를 호출된다.

3) Target Found와 Target Not Found 하위절차를 포함하는 Find DSE 절차를 실행함으로써 목표대상의 명칭을 분석한다. 요구된 엔트리가 발견되고 적절하면 확인 단계를 계속한다. 명칭결정 동안 오류가 좌우되면 응답된다. 엔트리가

적절하지 못한 게 발견되면 단계 4)에서 계속한다.

4) Name Resolution Continuation Reference Procedure가 NRcontinuationList에 저장된 계속 참조의 리스트를 처리하기 위하여 호출된다. 이들 계속 참조를 처리하기 위하여 연쇄된 요구는 다른 DSA에 발행될 수도 있다. 이 때 오류의 경우 국부적으로 또는 DAP/DSP를 경유하여 직접 응답된다. 연쇄된 요구에 응답이 있으면 결과단계로 단계 5)로계속한다.

5) Result Merging Procedure가 수신된 연쇄된 결과와 국부결과를 결합시키기 위하여 호출된다. 연쇄된 결과가 끼워 넣어진 계속 참조를 포함하면 이들은 서비스 제어 및 국부 정책이 허용하거나 또는 그것을 요구하면 빨리 분석될 수도 있다. 이것은 추가적 연쇄된 요구가 발행될 수도 있다. 연쇄된 결과는 삽입된 계속 참조를 할 수도 있다. 결합된 결과는 호출자에게 응답되며 요구의 처리는 끝난다.

6) 동작이 수정 동작이면 단계 7)에서 계속한다.
동작이 single entry interrogation operation이면 단계 8에서 계속한다.
동작이 multiple entry interrogation operation이면 단계 9에서 계속한다.
modification procedure를 실행할 때, 동작상의 결합은 확정, 수정, 종료되는 데에 필요할 수도 있으며 또는 새도는 동작이행의 결과로 갱신되는 데에 필요할 수도 있다. 이들이 원래의 동작의 이행을 동기적/비동기적으로 되느냐는 각각의 수정동작에 따른다. 국부 또는 DAP/DSP결과 또는 오류는 호출자에게 응답된다.

8) single entry interrogation operation의 결과는 국부 또는 DAP /DSP결과와 같이 호출자에 직접 응답된다.

9) 동작이 multiple entry interrogation operation이면 동작의 nameResolutionPhase를 점검한다. 그것이 completed가 아니면 List(I)또는 Search(I)절차를 호출한다. 그렇지 않으면 List(II)또는 Search (Ⅱ)절차를 각각 호출한다.

10) List(II)절차에 대한 결과 또는 오류와 List (I)절차에 대한 결과/오류의 성과는 호출자에게 직접 응답될 수 있다.
호출된 절차가 List (I)절차이었으면 결과는 역참조 되어야 하는 계속 참조를 포함하여야한다. 각각의 DSA에 보내어지는 연쇄된 리스트 동작을 초래할 수 있고, 결과 결합은 Result Merging Procedure에 대한 결과/오류로서 단계 5)에서 계속한다.

11) 동작이 탐색동작이었다면 모든 계속 참조는 Search Continuation Reference Procedure에 의하여 분석된다. 각각의 DSA에 보내지는 연쇄된 탐색요구를 일으킬 수도 있다. Result Merging Procedure는 탐색결과를 결합하기 위하여 그리고 포함된 계속 참조를 역참조 할 수도 있도록 호출된다.

2.3.1 요구확인절차

요구확인절차는 국부명칭 결정을 수행하기 전에 루프점검, 한계점검 및 보안점검을 수행하기 위하여 호출된다. 이 절차는 DUA로부터 온 요구인 경우 DAP에 의하여 제공되지 않은 chaining -Argument의 파라미터를 대한 생략설정을 제공한다. 또한 이 절차는 모든 포기요

구를 선택하고 이것을 동작 실행자에게 보고한다.

2.3.2 포기절차

포기절차는 포기되고 종료되는 동작을 시도하고, 만일 미해결의 하위 요구가 있으면 Chained Abandon동작을 뒤에 호출할 수도 있다. 절차는 호출자에게 Null Result를 응답하거나 tooLate문제를 가진 AbandonError 같은 오류 표시를 응답한다.

2.3.3 Find DSE 절차

Find DSE 절차에서는 목표 대상명을 도출하기 위해서 국부적으로 유지된 DSE에 대하여 목표 대상의 명칭요소에 일치시킨다. 별명 DSE가 만나게 되면 별명은 역참조되고, 정책적으로 허용이 되면 이 절차는 새로운 이름을 도출하기 위하여 재출발된다. 목표가 발견되지 못했으면 절차는 Target Not Found sub-procedure에서 계속된다. 목표가 발견되었으면 절차는 Target Found sub-precedure에서 계속된다. Target Not Found 및 Torget Found는 Find DSE절차의 계속이다. 만약 오류가 발생되면, 결합된 프로토콜 오류는 요구자에게 응답되며 동작 실행자는 종료된다.

Target Not Found sub-procecure는 Find DSE절차동안 검출되어진 지식 참조에 근거된 NRcontinuationList에서 continuationReferences 세트를 생성하며 DSE의 평가를 수행한다. 이 참조 세트는 Name Resolution Continuation Reference절차 내에서 계속 처리된다. 오류가 발생하면 결합된 오류는 요구자에게 응답되며 동작 실행자는 종료된다.

Target Found sub-procedure는 발견된 DSE가 요구된 동작에 대하여 적합하면, 즉 새도된 정보일 경우 점검한다. 이것은 하위트리 탐색과 같은 다중 대상 동작의 경우 목표 대상 하위의 새도된 정보의 전체 하위트리의 적합성 점검을 포함할 수도 있다. 엔트리가 적합하면 적절한 동작평가 절차가 시도되고, 그렇지 않으면 master에 향하는 continuationReference는 NRcontinuation List에서 생성되며 Name Resolution Continuation Reference절차가 시도된다.

2.3.4 단일 엔트리 호출 신호 절차

단일 엔트리 호출 신호 절차는 Read및 Compare와 같이 단일 엔트리에만 영향을 주는 동작을 실제로 실행하도록 시도된다. 실행후 절차에 의하여 생성된 결과/오류는 요구하는 DUA/DSA에 응답된다. 수정절차는 Addentry, RemoveEntry, ModifyEntry및 ModifyDN처리에 실행된다. 이것은 각각의 이들 동작에 대하여 정의된 특정 하위 절차를 실행함으로써 이루어진다. 이들 하위 절차 동안 DSP와 DISP 요구는 다른 DSA에게 지급될 수도 있다. 실행이 성공한 후 결과는 요구하는 DUA /DSA에 응답된다.

2.3.5. 다중 엔트리 호출신호 절차

다중 엔트리 호출신호 절차는 동일 DSA에 위치되거나 또는 분산되게 위치한 다중 엔트리에 영향을 주는 동작을 처리하도록 실행된다. 이것은 요구분석을 하도록 각각의 Search와 List동작에 대하여 정의된 특정 하위 절차를 실행함으로써 이루어진다. 이들 절차는 동작평가의 국부결과를 생성하며 SRcontinuationList에서 계속 참조 세트를 선택적으로 생성한다. SRcontinuationList가 이 절차의 마지막에 공집합이면 생성된 결과는 요구하는 DUA/DSA에 직접 응답된다. 그렇지 않으면 이들 계속 참조는 동작 유형에 따르는 List 또는 Search Continuation Reference절차를 계속함으로써 처리된다.

2.3.6 명칭결정 계속참조절차

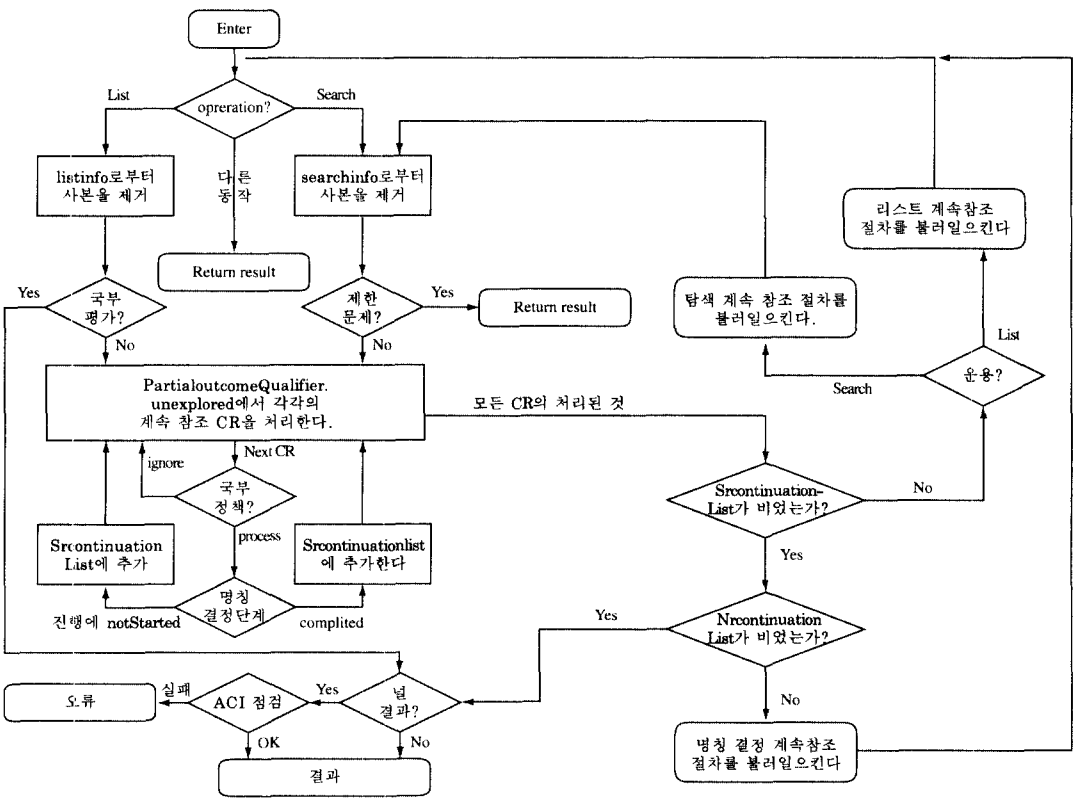
명칭결정 계속참조절차는 명칭 도출 단계동안 생성된 NRcontinuationList에서 계속 참조를 처리한다. 이들 연속 참조는 리퍼럴 오류에서 응답된 또는 연쇄된 하위요구를 발행하기 위하여 사용한다. 연쇄의 경우 연쇄된 요구로부터 응답된 결과/오류는 Result Merging절차에 의한 이후에 처리된다.

2.3.7 리스트 및 탐색 계속참조절차

리스트 및 탐색 계속참조절차는 다중 엔트리 호출신호 절차에 의하여 생성된 SRcontinuation-List에서 계속 참조를 처리하며, 연쇄된 하위요구 발행에 의하여 또는 partialOutcomeQualifier.unexplored내의 연속 참조 생성에 의하여 분석한다. 모든 미해결의 하위요구에 대하여 결과 또는 오류가 수신되면 Result Merging절차에 의하여 이후 처리를 위하여 응답된다.

2.3.8 결과 합체 절차

결과 합체 절차는 연쇄된 요구로부터의 결과를 시험하거나 또는 연쇄된 하위 요구로부터 수신된 결과와 함께 국부동작 결과를 결합시킨다. 하위요구가 오류를 응답했으면 이 오류가 어떻게 처리되어야 하느냐를 결정하게 된다. 결과에서 남겨진 계속 참조가 있으면 Name Resolution List/Search Continuation Reference 절차에 의하여 역참조될 것이다. 결합된 결과/미해결의 계속 참조는 요구하는 DUA/DSA에 응답한다.



〈그림 9〉 결과결합 절차

3. 디렉토리 서비스를 위한 프로토콜

디렉토리 서비스를 위한 프로토콜들의 설명은 X.519에 권고되어 있다. 디렉토리 프로토콜은 ROS-기반 응용 프로토콜의 규격에서 유용한 여러 개의 정보 객체 부류를 정의한다. ROS-OBJECT-CLASS는 OSI 통신 서비스를 사용하는 것이 실현될 때, ROS 객체는 응용 콘텍스트에 대해 응용 프로세스 및 약정에 매핑한다. 용어 추상 서비스는 ROS 결합 약정에 조회하고 있고 OSI 응용 계층 프로토콜은 OSI 통신 서비스를 사용하여 두 개의 개방 시스템간에 약정의 실현을 조회하고 있다. OPERATION-PACKAGE는 수요자 역할을 나타내는 ROS 객체에 의하여 요구되어질 수 있는 한 세트의 동작을, 공급자 역할을 나타내는 ROS 객체에 의하여 요구되어질 수 있는 동작, 양쪽의 ROS 객체들에 의해서 요구되어질 수 있는 동작을 정의한다.

CONNECTION-PACKAGE는 결합을 설정하고 복구하는데 사용된 결속 및 비결속 동작을 정의한다. OSI의 통신 서비스를 사용할 때 접속 패키지는 결합제어 서비스 요소의 서비스를 사용하는 절차로서 실현된다. CONTRACT는 접속 패키지 및 하나 또는 그 이상의 운용 패키지에 관해서 결속 약정을 정의한다. 약정을 규정할 때, 결합 개시자가 수요자의 역할을 하든지 결합 응답자가 수요자의 역할을 하든지 수요자의 역할을 하는 패키지를 나타낸다. APPLICATION-CONTEXT는 응용 콘텍스트의 정적 측면을 정의한다. 응용 콘텍스트를 거쳐 실현되는 약정, 결속을 설정하고 복구하는 OSI 서비스, 약정의 상호작용에 대하여 정보전송을 제공하는 OSI 서비스, 그리고 사용된 추상구문을 포함한다. ABSTRACT-SYNTAX는 ASN.1에 구추되어 있고, 그 값이 추상구문을 포함하는 ASN.1 유형에 객체 식별자를 정의한다. 디렉토리 규격, DAP, DOP, DISP 및 DOP에서 정의된 OSI 응용 계층 프로토콜은 한 쌍의 응용 과정들간의 통신을 제공하는 프로토콜이다. OSI 환경에서 표현 서비스를 사용하는 한 쌍의 응용 실체들간의 통신으로 표현된다. AE의 기능은 한 세트의 응용 서비스 요소들에 의하여 제공되어진다. AE들간의 상호 작용은 ASE에 의해 제공되어진 서비스의 사용 형식으로 기술된다. 디렉토리에 의하여 제공된 모든 서비스는 단일 AE에 포함된다. 원격 운용 서비스 요소는 운용의 요구 및 응답을 지원한다. 디렉토리 ASE는 ROSE에 의하여 제공된 서비스에서 디렉토리 운용 패키지 추상 구문 기호법에 관한 매핑기능을 제공한다. 결합 제어 서비스 요소는 한 쌍의 AE들간에 응용 결합의 설정 및 복구를 지원한다. DUA와 DSA간의 결합은 DUA에 의해서만 설정되어질 수 있다.

선택적으로 고신뢰 전송 서비스 요소는 DISP의 응용 프로토콜 데이터 유니트를 신뢰성이 있게 전송하고 있다.

3.1 용어정리

본 논문에서 사용되는 약어는 다음과 같다.

AC (Application Context) 응용 콘텍스트
ACSE (Association Control Service Element) 결합 제어 서비스 요소
AE (Application Entity) 응용 실체
APCI (Application protocol Control Information) 응용 프로토콜 제어 정보
APDU (Application Protocol Data Unit) 응용 프로토콜 제어 정보
ASE (Application Service Element) 응용 서비스 요소
DAP (Directory Access Protocol) 디렉토리 액세스 프로토콜
DISP (Directory Information Shadowing Protocol) 디렉토리 운용 결합 관리 프로토콜

DOP (Directory Operational Binding Management Protocol) 디렉토리 운용 결합 관리 프로토콜

ROS (Remote Operational Service) 원격 운용 서비스

ROSE (Remote Operations Service Element) 원격 운용 서비스 요소

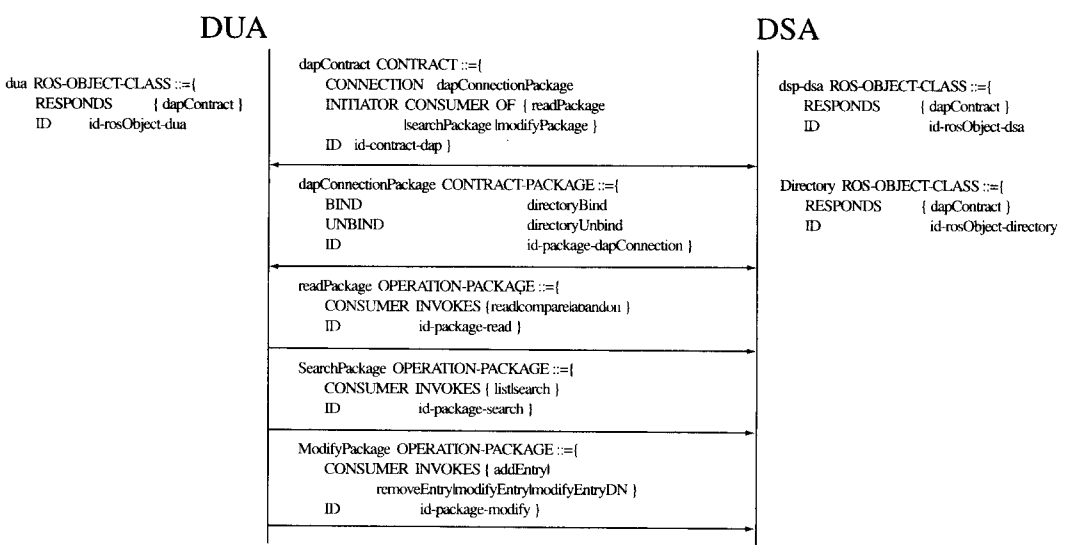
2.2 디렉토리 프로토콜

DAP, DSP, DOP 및 DISP 프로토콜은 다음과 같은 기초적 서비스를 사용한다.

- ROSE 서비스의 사용
  디렉토리 ASE는 ROSE의 RO-INVOKE, RO-RESULT, RO-ERROR, RO-REJECT-U와 RO-REJECT-P의 사용자이다. DAP와 DSP의 원격 운용은 비동기적이다. DUA가 DAP의 사용자일 때는 동기방법으로 동작하도록 선택될 수 있다. DISP의 원격 운용은 동기 운용으로 지원되어져야 하고 선택적으로 비동기 운용으로 지원되어질 수 있다. DOP의 원격 운영은 비동기이다.
- RTSE 서비스의 사용
  RTSE는 응용 프로토콜 데이터 유니트의 신뢰성 전송을 위해 준비한다. RTSE는 각 APDU가 정확하게 한 번 완전히 전송되어지는 또는 송출기가 예외를 경보하는 것을 보장한다. RTSE는 정상모드에서 사용되어진다. RTSE의 정상모드 사용은 ACSE의 정상모드 및 표현 서비스의 정상모드사용을 의미한다. 만약 RTSE가 응용 콘텍스트에 포함되어지면, RO-BIND 서비스는 RTSE의 RT-OPEN 서비스에서 매핑되고, RT-UNBIND 서비스는 RTSE의 RT-CLOSE에서 매핑된다. 기본 ROSE 서비스는 RTSE의 RT-TRANSFER, RT-TURN-PLEASE, RT-TURN-GIVE, RT-P-ABORT 및 RT-U-ABORT 서비스의 단독 사용자이다.
- ACSE 서비스의 사용
  ACSE는 AE들간의 응용 결합의 제어인 설정, 해제, 포기를 위하여 제공한다. 만약 RTSE가 응용 콘텍스트에 포함되어 있다면 그 RTSE는 ACSE의 A-ABORT 및 A-P-ABORT 서비스의 사용자이다. DAP를 지원하는 결합에서 A-ABORT 또는 A-P-ABORT의 수신은 모든 요구 프로세스를 종결시킨다. ITU-T 권고 X.518|ISO/IEC 9594-4에 기술된 어떤 조건에 대한 것을 제외하고는 이것은 DSP에 대해서 역시 사실이다. 만약 DIB에 대한 요구된 수정이 생기는지를 확인하는 것은 디렉토리 사용자의 책임이다.
- 표현 서비스의 사용
  표현 계층은 교환되어져야 하는 응용 계층 내용의 구문을 조정한다. 정상모드에서 다른 표현 콘텍스트에 응용 콘텍스트에 포함된 각 추상구문에 사용되어진다. 만약 RTSE가 응용 콘텍스트에 포함되어 있으면, RTSE는 표현서비스의 P-ACTIVITY-START, P-ACTIVITY-END, P-ACTIVITY, P -ACTIVITY-DISCARD, P-ACTIVITY-RESUME, P-DATA, P-MINOR-SYNCHRONIZE, P-U -EXCEPTION-REPORT, P-P-EXCEPTION-REPORT, P-TOKEN-PLEASE 및 P-CONTROL -GIVE 서비스의 단독 사용자이다. 만약 RTSE가 응용 콘텍스트에 포함되어 있지 않으면, ROSE는 표현 서비스의 P-DATA 서비스의 단독 사용자이다. 표현 디폴트 콘텍스트, 콘텍스트 복원, 콘텍스트 관리는 사용되지 않는다.

• 하위 계층 서비스의 사용
세션 계층은 단말 시스템들간에 정보의 흐름을 구성하고 있다. 전송계층은 기본 통신망 접속을 통해 단말간의 이동가능한 데이터 전송을 제공한다. 세션 계층에 의해 전송 서비스 등급의 선택은 다중화 요건 및 오류 회복 요건에 의해 좌우된다. 전송 등급 0의 부여 즉 비다중화는 필수적이다. 빠른 전송 서비스는 사용되지 않는다. 다른 등급의 부여는 선택적이다. 다중화 등급은 같은 통신망 접속을 통해 DAP 또는 DSP 및 다른 프로토콜을 다중화하는데 사용될 수도 있다. 오류 회복 등급은 허용할 수 없는 오류율이 가진 통신망 접속을 통해 선택될 수도 있다.

디렉토리 프로토콜에 사용된 두 개의 추상 구문을 다른 곳에서 규정되어진다. ACSE의 추상구문, acse-abstract-syntax은 결합을 설정하는데 필요하다. RTSE의 추상 구문, rtse-abstract- syntax는 DISP에 선택적으로 필요해진다. 추상 구문의 값이 획득된 ASN.1유형은 ROS{}, BIND{} 및 Unbind{}를 사용하여 규정되어진다. 이들의 추상 구문 및 그들의 규정된 아래의 것은 기본 ASN.1 부호화 규칙에 따라서 부호화되어져야 한다. 디렉토리 프로토콜에 사용된 두 개의 추상 구문을 다른 곳에서 규정되어진다. ACSE의 추상 구문,acse-abstract-syntax은 결합을 설정하는데 필요하다. RTSE의 추상 구문, rtse-abstract-syntax는 DISP에 선택적으로 필요해진다. 추상 구문의 값이 획득된 ASN.1유형은 ITU-T 권고 X.880|ISO/IEC 9072-1에 정의된 파라미터화된 유형 ROS {}, BIND {} 및 Unbind{}를 사용하여 규정되어 진다. 이들의 추상 구문 및 그들의 규정된 것은 기본 ASN.1 부호화 규칙에 따라서 부호화되어져야 한다.



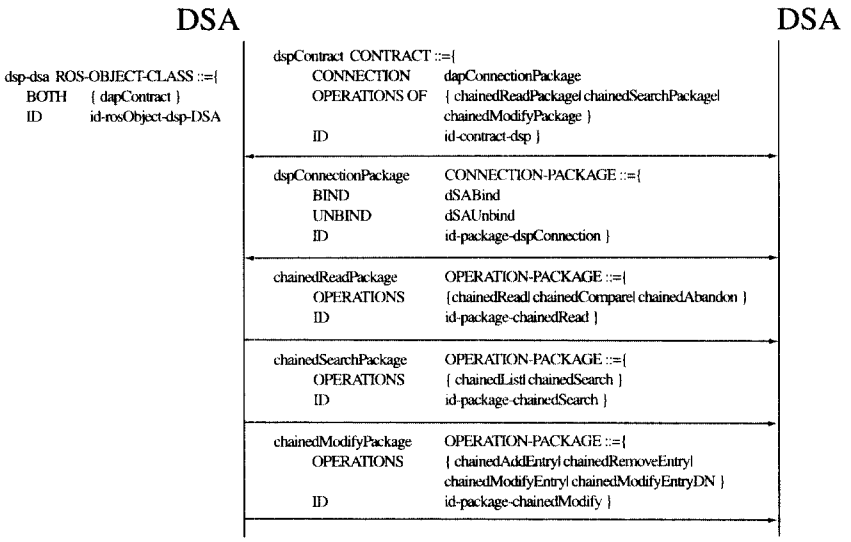
〈그림 10〉 Directory Access Protocol

2.2.1 DAP 추상 구문

운용 패키지를 실현하는 디렉토리 ASE는 단일 추상 구문, directoryAccessAbstract-Syntax를 공유한다. 이것은 부류 ABSTRACT-SYNTAX의 정보 객체로서 규정되어진다. 디렉토리 프로토콜에 사용된 두 개의 추상 구문을 다른 곳에서 규정되어진다. ACSE의 추상 구문, acse-abstract-syntax은 결합을 설정하는데 필요하다. RTSE의 추상 구문, rtse-abstract-syntax는 DISP에 선택적으로 필요해진다.

2.2.2 DSP 추상 구문

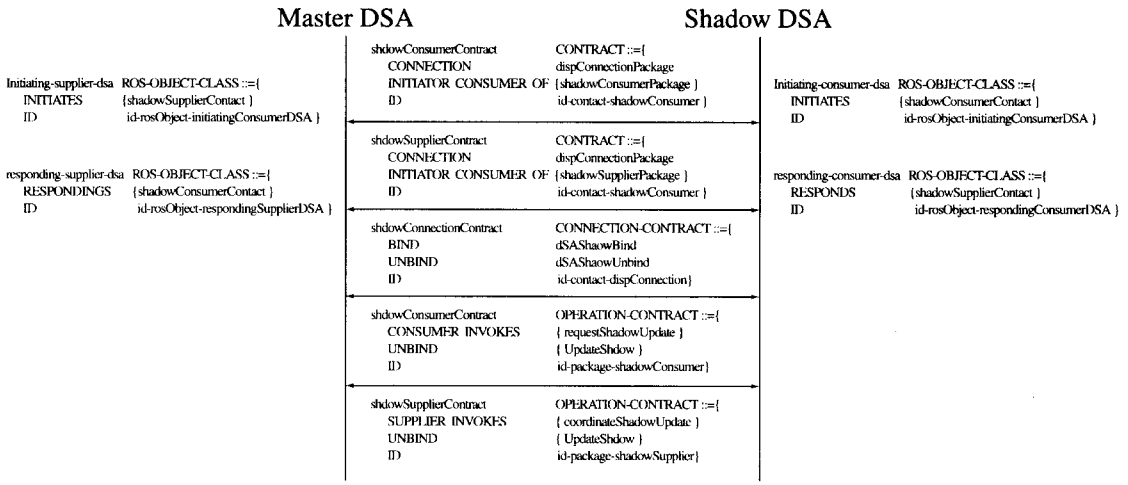
운용 패키지를 실현하는 디렉토리 ASE는 단일 추상 구문, directorySystemAbstract-Syntax를 공유한다. 이것은 부류 ABSTRACT-SYNTAX의 정보 객체로서 규정되어진다.



〈그림 11〉 Directory System Protocol

2.2.3 DISP 추상구문

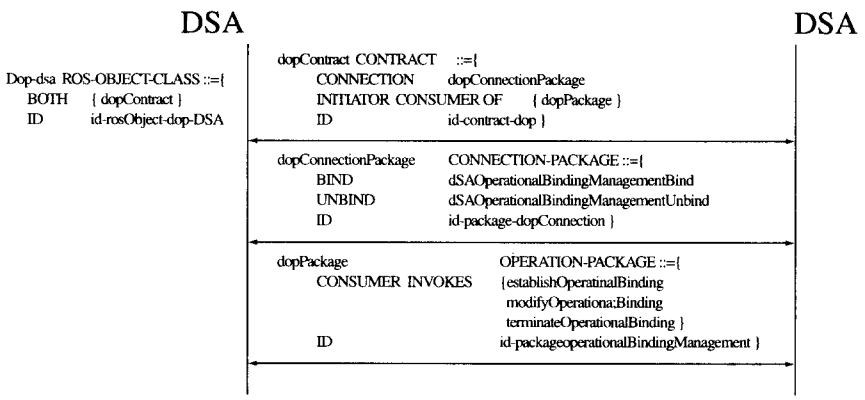
디렉토리 ASE는 응용 콘텍스트에서 사용되는지, 되지 않는지에 따라서 추상구문 directory -ShadowAbstactSyntax이거나, 또는 directoryReliableShadowAbstr actSyntax이다. 이들의 두 개 추상구문은 부류 ABSTRACT-SYNTAX의 정보 객체로서 규정되어진다. 추가로, 다음의 추상 구문은 RTSE를 사용한 콘텍스트에서 사용되어진다. 이것은 RTSE 자체의 추상구문과 Bind {dSAShadowBind} 및 Unbind{dSAShadowUnbind}의 추상구문을 포함한다. 추상구문의 값이 획득되어지는 ASN.1 유형은 ROS{}, Bind{}, 그리고 Unbind {} 파라미터화된 유형을 사용하여 규정되어진다.



〈그림 12〉 Directory Information Shadowing Protocol

2.2.4 DOP 추상 구문

운용 패키지를 실현하는 디렉토리 ASE는 추상 구문, directoryOperationalBinding Management-AbstractSyntax를 사용한다. 이것은 ABSTRACT-SYNTAX의 정보 객체로서 규정되어진다.



〈그림 13〉 Directory Operational Binding Management Protocol

2.3 디렉토리 응용 콘텍스트

디렉토리 응용 콘텍스트는 dapContract는 directoryAccessAC로서 실현되어진다. 본 응용 콘텍스트는 APPLICATION- CONTEXT의 정보 객체로서 규정되어진다. dspContract는 directory -SystemAC로서 실현되어진다. 본 응용 콘텍스트는 APPLICATION- CONTEXT의 정보 객체로서 규정되어진다. 만약 DSA가 DISP를 지원하면, 그 DSA는 적어도 섀도 공급자 역할 또는 섀도 수요자 역할의 하나를 그리고 적어도 shadowSupplierInitiatedAC 또는 shadowConsumer -InitiatedAC의 하나를 지원하여야 한다. 만약 DSA가 특별한 역할을 위해서 shadowSupplierInitiatedAC를 지원하면, 이것은 또한 선택적으로 동일한 역할을 위해 reliableShadowSupplierInitiatedAC를 지원한다. 만약 DSA가 특별한 역할을 위해서 shadow-ConsumerInitiatedAC를 지원하면, 이것은 또한 선택적으로 동일한 역할을 위해 reliable-ShadowConsumerInitiatedAC를 지원한다. shadowSupplierContract는 shadowSupplier-InitiatedAC로 실현된다. 본 응용 콘텍스트는 APPLICATION-CONTEXT의 정보 개체로서 규정한다.

4. 결 론

전자상거래가 일부에서 이루어지고 있고, 전자서명을 위해서는 전자서명기술이 기반이 되어야 한다. 전자서명기술에서는 공개키 암호 알고리즘이 사용될 것이고 비밀키는 전자서명을 생성하는 생성키로, 공개키는 전자서명을 검증하는 검증키로 사용된다. 그러므로 전자서명기술은 서명키와 검증키 즉 비밀키와 공개키의 관리가 중요하다. 비밀키는 안전하게 보관되어야 하고 공개키는 공개되는 정보이므로 공개키의 인증이 필요하다. 이를 위해서는 전자인증제도가 마련되어야 하고 인증서를 발급하기 위한 인증기관이 필요하다. 인증제도를 위한 법·제도의 제정과 개정이 요구되고 기술적으로는 공개키 기반 구조가 구축되어야 한다. 특히 공개키 기반구조를 위한 디렉토리 서비스는 필수불가결한 요소이다.

본 논문에서는 이러한 디렉토리 서비스 표준안인 X.500 시리즈 중 X.518과 X.519를 알아보았다. X.518은 분산된 디렉토리 응용에 참여하는 DSA의 동작을 규정하고, DIB가 많은 DSA를 통하여 광범위하게 분산된 환경하에서 일관성있는 서비스를 보장하기 위해 설계된 것이다. X.519는 추상서비스를 이행하는 디렉토리 액세스 프로토콜, 디렉토리 시스템 프로토콜, 디렉토리 정보 섀도 프로토콜, 디렉토리 운용 결합 관리 프로토콜을 설명한다.

이렇게 전자결재, 전자서명, 전자인증과 전자상거래등의 세계적인 움직임속에서 우리나라에서도 정보통신부와 한국정보보호센터가 기반기술 마련을 추진중이다. 또한 한국형 전자서명인 KCDSA가 표준화 추진중이고, 현재는 공개키 기반구조를 구축, 전자인증제도를 마련하고 인증기관들의 통합·관리를 위한 기관이 요구된다.

참 고 문 헌

[1] 최성민, 이인숙, 장청룡, 원동호, "분산디렉토리 시스템에서 인증에 관한 연구", 한국통신정보보호 학회 학술 발표회 논문집, pp. 41-54, 1992

[2] ITU-T Recommandation X.500 (1993) |ISO/IEC 9594-1:1993, Information technology - Open Systems Interconnection - The Directory:Overview of Concepts, Models and Services, 1993.

[3] ITU-T Recommandation X.501 (1993) |ISO/IEC 9594-3:1993, Information technology - Open Systems Interconnection - The Directory:Abstract Service Definition, 1993.

[4] ITU-T Recommandation X.511 (1993) |ISO/IEC 9594-3:1993, Information technology - Open Systems Interconnection - The Directory:Abstract Service Definition

[5] ITU-T Recommandation X.518 (1993) |ISO/IEC 9594-4:1993, Information technology - Open Systems Interconnection - The Directory:Procedures for Distributed Operation, 1993.

[6] ITU-T Recommandation X.519 (1993) | ISO/IEC 9594-5:1993, Information technology - Open Systems Interconnection - The Directory:Protocol Specifications, 1993.

[7] ITU-T Recommandation X.520 (1993) |ISO/IEC 9594-6:1993, Information technology - Open Systems Interconnection - The Directory:Selected Attribute Types, 1993.

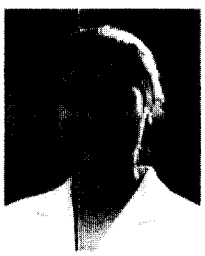
[8] ITU-T Recommandation X.521 (1993) |ISO/IEC 9594-7:1993, Information technology - Open Systems Interconnection - The Directory:Selected Object Classes, 1993.

[9] ITU-T Recommandation X.509 (1993) |ISO/IEC 9594-8:1993, Information technology - Open Systems Interconnection - The Directory:Authectication Framework, 1993.

[10] ITU-T Recommandation X.525 (1994) |ISO/IEC 9594-9:1993, Information technology - Open Systems Interconnection - The Directory:Replication, 1993.

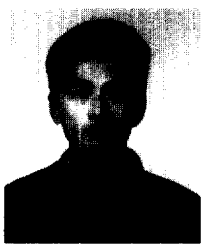
[11] 이재광, 이용준, "X.500 디렉토리 정보보호", 통신정보보호학회지, 4권 3호, pp. 22-33, 1994. 9.

□ 著者紹介



정 윤 정

1975년 1월 21일생
1997년 8월 성균대학교 수학과 졸업(이학사)
1997년 3월 ~ 현재 성균관대학교 전기전자컴퓨터공학부 석사과정



김 준 태

1990년 3월 ~ 1997년 2월 성균관대학교 정보공학과 졸업(공학사)
1997년 3월 ~ 현재 성균관대학교 전기 · 전자 및 컴퓨터공학부 석사과정

오 수 현

1974년 10월 16일생
1998년 2월 성균관대학교 정보공학과 졸업(공학사)
1998년 3월 ~ 현재 성균관대학교 전기전자컴퓨터공학부 석사과정

정 병 천

1974년 6월 12일생
1998년 2월 성균관대학교 정보공학과 졸업(공학사)
1998년 3월 ~ 현재 성균관대학교 전기전자컴퓨터공학부 석사과정

원 동 호

1976년 2월 성균관대학교 전자공학과 졸업(공학사)
1978년 2월 성균관대학교 대학원 졸업(공학석사)
1988년 2월 성균관대학교 대학원 전자공학과(공학박사)
1978년 4월 ~ 1980년 3월 한국전자통신연구소 연구원
1985년 9월 ~ 1986년 8월 일본 동경 공대 객원 연구원
1982년 3월 ~ 현재 성균관대학교 공과대학 정보공학과 교수
1991년 ~ 현재 한국통신정보보호학회 편집이사
1996년 4월 ~ 현재 정보화추진위원회 자문위원

※ 주관심 분야 : 암호이론, 정보이론