

졸업작품 보고서

# 스마트카드를 이용한 통합 인증 관리 시스템

SPs.

90012641	조상호
90112594	이운남
90011647	김유신
90011544	김상권
90011960	서재휘
90011635	김원섭
90111796	김중대

2006. 11.

중부대학교 정보보호학과  
지도교수 : 이병천

## 구축 배경

최근 개인 정보 보호에 관한 법률의 정비가 급속히 진행되고 있다. 특히 주목받고 있는 개인 정보 보호법 에서는 개인정보를 수집/관리하는 시스템의 소유자는 정보를 제공하는 개인에 대해 보안의 위탁이 요구되고 있다.

기업에서도 보안 의식의 고양이나 네트워크 이용의 확대에 따라서 강력한 보안을 보관 유지하는 한편 편리성이 높은 개인 인증 시스템이 요구되고 있기 때문에 확실한 개인 인증의 실시는 정보 누설 방지 및 불법 변경 방지 대책으로서도 중요시되고 있다.

또, 네트워크 보안을 생각하는데에 답이 되는 것은 인증이다. 인정 방법으로는 패스워드를 이용한 인증이 가장 일반적이다. 그러나 패스워드를 이용한 인증은 기억하기 쉽고 간단한 문자열을 패스워드로서 설정하는 경우가 많으며 타인에게 알려줌으로써 본인 이외의 여러 사람으로부터의 동시 이용이 가능하기 때문에 보안면에서 보면 매우 취약하다. 이러한 취약성을 해결하기 위해서 다양한 인증 방법이 실용되고 있다.

예를 들면 OTP(One Time Password)나 토큰, 스마트카드 등이 있다. 이러한 인증 방법은 그 어떤것을 보관 유지하고 있는 것과 비밀번호를 통한 제2요소 인증이다.

이러한 방법으로 기존의 패스워드 로그인에 한차원 업그레이드된 보안을 제공 받을 수 있다. 이에 우리는 스마트카드와 USB토큰을 이용한 인증 방식을 기술하게 되었다.

## 요약

본 졸업작품에서는 스마트카드를 이용한 통합 인증 시스템을 구현하였다.

본사의 AD서버가 타 지역에 있는 지사의 클라이언트들 까지 직접 인증 관리를 할 필요없이 지사의 AD서버에게 본사 AD서버의 인증 관리 권한을 똑같이 부여한다. 이는 곧 지사 클라이언트의 인증을 지사 AD서버가 하위 인증 기관으로서 인증하게 되는 것이다.

본사와 지사의 서버 관리자는 스마트카드를 이용해 개인 인증으로 서버에 접근 및 각각의 클라이언트에게 인증 요청을 받아 인증해 줄 수 있다. 또한 스마트카드와 마찬가지로 IC칩이 내장된 USB토큰을 이용하여 보안 인증 권한을 줄 수 있다. 이는 서버에 AD를 구축하여 각 클라이언트에게 인증 권한을 부여할 수 있다.

이처럼 우리는 하나의 회사 안에 상위 인증 서버와 하위 인증 서버를 구축하여 클라이언트를 분리하여 인증 권한을 부여하는 시스템을 구축하여 보았다. 이로써 단순한 패스워드 인증 방식을 넘어 차세대 인증 방식인 스마트카드와 USB토큰 인증을 구현하였다.

본론에서도 소개하겠지만 스마트카드는 PIN 넘버 방식으로 이중 인증 중에서도 많이 사용되고, 안정적이고, 비용 효율적인 형태이다. 적절하게 관리한다면, 스마트카드를 가지고 있고 암호를 아는 사용자만 네트워크 리소스 액세스 권한을 획득할 수 있다. 이중 요구 사항은 조직의 네트워크에 대한 무단 액세스 가능성을 현저하게 감소시킬 수 있다. 이로 인해 효과적인 보안 제어를 제공 받을 수 있고, 관리자 계정 보안 및 원격 액세스 보안이 가능하다. 이는 IC칩에 내장되는 인증 방식을 이용하여 보다 확실한 보안 인증 및 관리가 가능하다.

# 목차

1. 서론 .....	9
1.1 인증 시스템 .....	9
1.1.1 인증 시스템의 배경 .....	9
1.1.2 보안 인증 메커니즘의 필요성 .....	9
1.1.3 보안 인증 메커니즘의 구현 방식 .....	10
1.2 인증이란 무엇인가 .....	10
1.3 인증의 요구사항 .....	10
1.4 인증 기술의 필요성 .....	11
2. 주요 기반 기술 .....	12
2.1 ACTIVE DIRECTORY .....	12
2.1.1 ACTIVE DIRECTORY란 무엇인가 .....	12
2.1.1.1 디렉토리 서비스 기능 .....	12
2.1.1.2 중앙화된 관리 .....	12
2.1.1.2-1 보안 그룹 .....	13
2.1.1.2-2 그룹 정책 .....	13
2.1.2 ACTIVE DIRECTORY의 구조 .....	13
2.1.2.1 논리적 구조 .....	13
2.1.2.2 물리적 구조 .....	15
2.2 SMART CARD .....	15
2.2.1 SMART CARD란 무엇인가 .....	15
2.2.2 SMART CARD의 내부 구조 .....	16
2.2.3 SMART CARD 사용의 기대 효과 .....	16
2.3 USB TOKEN .....	17
2.3.1 USB TOKEN이란 무엇인가 .....	17
2.3.2 USB TOKEN의 효과 .....	17
3. 인증 시스템의 필요 기술 .....	18
3.1 ACTIVE DIRECTORY .....	18
3.2 SMART CARD 및 USB TOKEN (물리적 인증 도구) .....	18
3.3 시스템 환경 .....	18
3.3.1 환경 구축을 위한 구성 요소 .....	18

3.3.2 환경 구축을 위한 시스템 기반 구조 .....	19
4. 인증 시스템의 기술적 구현 및 사용 방법 .....	21
4.1 ACTIVE DIRECTORY의 구현 .....	21
4.1.1 ACTIVE DIRECTORY 설치 .....	21
4.1.2 엔터프라이즈 관리자 계정 변환 .....	24
4.1.3 IIS 설정 .....	26
4.1.4 엔터프라이즈 루트 CA설치 .....	27
4.1.5 하위 CA 설치 .....	32
4.1.5-1 하위 인증CA 권한부여 .....	34
4.2. SMART CARD의 구현 .....	35
4.2.1 SMART CARD 시스템의 구현 단계 및 시스템 통합 과정 .....	35
4.2.2 SMART CARD 설치 .....	35
4.2.2-1 스마트카드를 사용한 관리자 계정 보호 .....	35
4.2.3 CSP(Cryptographic Service Provider) 설치 절차와 방법 .....	35
4.2.3.1 CSP 설치절차 .....	36
4.2.3.2 CSP 설치방법 .....	37
4.2.4 인증서 신청 절차 및 방법 .....	38
4.2.4.1 스마트카드 인증서 신청 절차 .....	38
4.2.4.2 인증서 발급 절차 .....	41
4.2.4.3 인증서 사용 및 적용방법(WEB) .....	42
4.3 USB TOKEN의 구현 .....	43
4.3.1 USB TOKEN .....	43
4.3.2 USB 토큰용 인증서 준비과정 .....	43
4.3.3 등록된 USB토큰 사용방법 .....	47
4.3.4 Web에서 인증서 발급 절차 .....	49
5. 결과 및 분석 .....	52
5.1 통합 인증 관리 시스템의 동작 과정 .....	52
6. 결론 .....	53
7. 참고문헌 .....	54

## 그림 목차

<그림 1. 스마트 칩의 내부>.....	8
<그림 2. AD 설치준비>.....	13
<그림 3. AD 설치> .....	13
<그림 4. 도메인 지정> .....	14
<그림 5. NetBIOS 도메인명 지정>.....	14
<그림 6. DNS등록 진단> .....	15
<그림 7. IP 설정>.....	15
<그림 8. 복원모드 암호설정>.....	16
<그림 9. AD사용자 및 컴퓨터>.....	16
<그림 10. 관리자 속성>.....	17
<그림 11. AD 관리자 세부설정>.....	17
<그림 12. IIS 서비스 설정> .....	18
<그림 13. IIS서비스 속성 선택>.....	18
<그림 14. IIS 서비스 구성 완료> .....	19
<그림 15. 엔터프라이즈 루트 CA 설치>.....	19
<그림 16. CA 설치 알림 창>.....	19
<그림 17. 인증서 DB 설정> .....	20
<그림 18. 인증서 템플릿 추가>.....	20
<그림 19. 사용할 인증서 템플릿 선택> .....	20
<그림 20. 추가된 인증서 템플릿>.....	21
<그림 21. 새 도메인 컨트롤러 선택>.....	21
<그림 22. 자식 도메인 선택>.....	21
<그림 23. 도메인 컨트롤러 사용자 설정>.....	22
<그림 24. 도메인명 설정>.....	22
<그림 25. NetBIOS 이름 선택>.....	22
<그림 26. DNS 등록 진단> .....	23
<그림 27. 사용 권한설정>.....	23
<그림 28. 옵션 확인> .....	23
<그림 29. AD설치 완료> .....	24
<그림 30. CA설치> .....	24

<그림 31. 하위 CA>·····	24
<그림 32. 하위 CA 이름입력> ·····	25
<그림 33. 하위 CA 인증서 요청> ·····	25
<그림 34. 인증서 발급확인> ·····	25
<그림 35. CA 설치 완료>·····	26
<그림 36. 권한부여>·····	26
<그림 37. 상세 권한 설정>·····	26
<그림 38. 카드리더기 설치화면>·····	28
<그림 39. CSP설치 메뉴화면> ·····	28
<그림 40. 신화 CSP 설치화면>·····	29
<그림 41. 신화 CSP 사용자명과 제품 키 입력> ·····	29
<그림 42. 스마트카드 인증서 요청> ·····	30
<그림 43. 스마트카드용 인증서 종류 선택>·····	30
<그림 44. 암호화 서비스 공급자 선택> ·····	31
<그림 45. 스마트카드 인증서 요청 완료>·····	31
<그림 46. 스마트카드 PIN 입력>·····	31
<그림 47. Web에서의 스마트카드 인증서 신청 화면> ·····	32
<그림 48. Web에서의 스마트카드 인증서 요청> ·····	32
<그림 49. WEB에서의 스마트카드 인증서 요청> ·····	32
<그림 50. Web에서의 스마트카드 인증서 등록 스테이션>·····	33
<그림 51. 스마트카드 인증서 발급> ·····	33
<그림 52. 발급된 스마트카드용 인증서 정보> ·····	33
<그림 53. 스마트카드 인식> ·····	34
<그림 54. 스마트카드 로그인> ·····	34
<그림 55. USB 토큰 작동확인>·····	35
<그림 56. 신규 USB토큰 스냅인 추가> ·····	35
<그림 57. 인증서 추가>·····	36
<그림 58. 관리될 인증서 대상 선택> ·····	36
<그림 59. 인증서 생성>·····	36
<그림 60. 개인 인증서 신청>·····	37
<그림 61. 인증서 요청 마법사>·····	37

<그림 62. 스마트카드 로그인 선택> .....	37
<그림 63. CSP 선택> .....	38
<그림 64. 사용할 인증기관 선택> .....	38
<그림 65. 인증서 요청>.....	38
<그림 66. 인증서 이름 및 설명 입력>.....	39
<그림 67. USB토큰 PIN번호 확인>.....	39
<그림 68. 네트워크 식별 마법사> .....	39
<그림 69. 네트워크 종류 선택> .....	40
<그림 70. 도메인 선택>.....	40
<그림 71. 사용자 계정 등록확인> .....	40
<그림 72. 사용자 계정 및 도메인 정보 확인>.....	40
<그림 73. 등록될 사용자 접근권한 선택>.....	41
<그림 74. 네트워크 식별 완료>.....	41
<그림 75. Web 접속> .....	41
<그림 76. USB토큰 인증서 요청>.....	42
<그림 77. 인증서 등록>.....	42
<그림 78. 사용자 선택>.....	43
<그림 79. 인증서 요청정보 입력 완료> .....	43
<그림 80. PIN 번호 입력>.....	43
<그림 81. 인증서 발급 및 설치 완료>.....	43
<그림 82. 통합 인증 관리 시스템의 구성> .....	44

## 표 목차

<표 1. 보안기술 요구사항> .....	3
<표 2. 스마트카드 보안그룹>.....	5
<표 1. 시스템 구축 사양 및 필요기술> .....	11



# 1. 서론

## 1.1 인증 시스템

### 1.1.1 인증 시스템의 배경

급변하는 디지털 정보사회는 눈부신 정보통신기술의 발달과 함께 우리 앞에 성큼 다가왔다. 이에 따라 정보시스템이 팔목할 만큼 성장하고 다양한 네트워크를 이용한 정보처리 요구와 접근이 급격히 증가하고 있으며, 아울러 정보보안 및 정보보호 문제가 날로 심각해지고 있다. 더불어 특정지역에의 출입통제를 위한 보안시스템의 필요성도 증대되고 있는 만큼 도난이나 위조의 문제점이 거의 없고 시대변화에 쉽게 적용되어 사용자의 신원을 확인·인증할 수 있는 방법이 요구되고 있는 것이다. 인증과정에서는 주로 인증 메커니즘이 사용되는데, 종래의 암호와 같은 인증방식의 경우 분실이 쉽고 타인에게 노출되기 쉬워 개인을 안전하게 인증하는 수단으로써 문제점이 있는 반면, IC칩이 들어간 스마트카드 및 USB 토큰 등은 현재 우리가 흔히 사용하고 있는 일반 계정으로 패스워드를 입력하여 로그인하는 방식과는 다르게 IC칩 안에 인증 기관의 인증서를 등록 받아 PIN번호를 입력하여 로그인하는 안전성있는 방식으로 정보에 접근한다. 또한 개인의 고유한 신체의 생리학적이고 행위적인 생체인식방식은 보안성이 우수하고 사용이 간편한 생체인식기술을 활용하는 방식도 있다. 이러한 응용분야들은 전자상거래인증시스템 등 인터넷보안시스템으로 점차 확산되는 추세에 발맞추어 정보의 접근성을 보다 안전하게 하고 있다. 더욱이 IC칩 기반의 접근 기술과 생체인증 시스템 기술들은 사회적으로 인정된 보안관련 기술 세계적인 주목을 받고 있다.

### 1.1.2 보안 인증 메커니즘의 필요성

인증 기술은 앞에서 말한것과 같이 급변하는 디지털 정보화 사회에 없어서는 안될 기술이다. 정보의 보호란 커다란 맥락 안의 한 부분인 인증 메커니즘은 개인의 정보를 자신이 아닌 타인이 그 정보에 대해 열어볼 경우와 보안성이 필요한 중요 기술에 대해 원천적으로 접근을 차단하고 회사내의 기밀 정보에 접근이 허용된 이들만이 접근 할 수 있도록 접근제어를 할 수 있도록 해야 한다. 또한 회사의 경우 정보에 있어서 정보를 공유할 사람들에 대한 권한을 따로 제어 할 수 있어야 한다. 이에 관리자는 자신이 만든 정책에 있어 인증 권한을 주어야 하며 비인증자에 대한 접근을 사전에 차단 할 수 있도록 해야 한다. 하지만 하드웨어에 인증서를 받는 방식은 타인이 컴퓨터에 접근하여 ID와 패스워드만 알고 있어도 접근이 허용된다. 또한 패스워드의 관리 소홀로 원치 않게 타인이 패스워드를 해킹하여 인증되지 않은 서버에 접근하여 정보를 해킹할 수 있다. 그러나 IC칩이 들어간 스마트카드와 USB 토큰은 하드웨어에 인증서를 받아 타인이 패스워드만 알아도 접근할 수 있는 경우와는 다르게 스마트카드를 따로 들고 다니며 해킹하기 어려운 IC칩에 인증서를 받아 접근하기에 일차적인 타인 접근이 어려운 것이다.

인증 방법에 있어서는 인증서의 발급이 있는데 기존의 하드웨어 저장 인증 방법보다 체계적이고 안전한 IC칩이 들어있는 스마트카드 및 USB 토큰, 생체 인식등의 인증 방식이 필요하다. 스마트카드의 경우 카드 내에 들어있는 IC칩은 실제로 인증서를 기존 하드에 저장하는 방식보다 타인의 접근성을 줄일 수 있으며 IC칩 내의 안전한 설계로 인해 위조 및 변조 등 접근 해킹 및 오남용을 어렵게 하여 타인의 로그인을 방지 할 수 있다. 또한 USB토큰은 스마트카드를 리더기로 읽어들이어 로그인 하는 방식과 다르게 USB 토큰의 설치 프로그램만 설치하면 리더기가 필요없이 보안 인증이 가능하다.

### 1.1.3 보안 인증 메커니즘의 구현 방식

이에 우리는 앞에서 말한것과 같이 기존의 방식보다 정보의 접근을 까다롭게할 IC칩이 내장된 스마트카드와 USB 토큰 인증 방식을 구현할 것이다. 또한 정보에 대한 접근 권한을 가상의 사내 망으로 구현하여 부여하는 방식으로 할 것이다. 먼저 사 내의 서버를 구축하고 인증 서버를 구성하여 각각의 사내 사용자(클라이언트)들에 대한 인증 부여및 접근 제어를 재현해 볼 것이다. 또한 사내 망이 커짐에 따라 지사를 두어 지사의 서버에 하위 인증 권한을 주어 지사 서버에 연결된 사용자(클라이언트)들에 대한 인증 부여 권한을 주어 지사 자체로서 본사와 같은 구성을 나타낼 것이다.

최초로 인증이란 무엇인지 간략하게 살펴본 후 최초로 구성될 서버(Windows 2003 Server)를 구축하고 그 위에 서버를 통합 관리하기 위한 Active Directory 기술의 설명 및 설치와 설정, 그리고 인증 메커니즘인 스마트카드와 USB토큰이 왜 필요한지 그리고 이것의 인증 방식을 설치하여 하위 인증 기관의 권한 부여 방식과 각각의 사내 사용자(클라이언트)들의 인증 부여 방식을 가상으로 구성하여 설정할 것이다.

## 1.2 인증이란 무엇인가

인증이란 인터넷이라는 불안정하고 개방적인 가상공간에서 사용자의 신원을 확인하고 거래의 안전을 확보하기 위한 방법으로 전자서명 검증키가 사용자가 소유한 전자서명 생성키에 일치한다는 사실을 공신력 및 전문성을 갖춘 인증기관이 확인, 증명하는 것을 말한다.

## 1.3 인증의 요구사항

전자거래를 안전하게 하기 위한 보안 요구사항은 크게 인증(Authentication), 무결성(Integrity), 비밀성(Confidentiality) 및 부인봉쇄(Non-Repudiation) 등 4가지로 분류할 수 있다.

### i. 인증(Authentication)

- 자신의 신분과 행위를 증명하는 것
- 위장, 스푸핑에 효과적으로 대응
- 사이버 공간에서 자신이 합법적이고 정당한 실체임을 나타내는 실체인증

- ex) 웹서버의 웹브라우저에 대한 인증
- 문서나 전자우편이 특정인에게서 온 것임을 증명하는 송신자 인증
- ex) 디지털 서명

#### ii. 무결성(Integrity)

- 문서나 메시지가 전달되는 과정에서 변조되지 않도록 실현하는 서비스
- 실제 서비스에서 무결성이 기밀정보보다 더욱 중요
- 문서 위조나 되돌이 공격(replay attack)의 위협에 대응

#### iii. 비밀성(Confidentiality)

- 제3자에게 노출되지 않는 기능
- 암호이론의 출발점
- 개인정보, 기밀자료에 대한 기밀의 확보

#### iv. 부인봉쇄(Non-Repudiation)

- 자신의 행위에 대한 부인
- 거래내역에 대한 부인
- 메시지 교환 자체에 대한 부인

위의 4가지 보안을 위한 요구사항을 충족하기 위한 기술은 다음과 같은 표로 정리해 볼 수 있다.

보안 요구사항	인증	무결성	부인봉쇄	비밀성
보안 기술	전자서명			암호화

<표 1. 보안기술 요구사항>

전자문서의 비밀성을 보장해 주는 기술이 암호화 기술이며, 전자서명 기술은 거래상대방의 신원확인, 거래내용의 위, 변조방지, 거래사실의 부인방지 등을 보장해 주는 기술인 것이다.

### 1.4 인증 기술의 필요성

인증이 왜 필요한가는 다음과 같이 요약된다.

- 불특정다수인의 전자 서명키 인증을 효율적으로 수행
- 전자 서명키 인증의 공신력 제고
- 전자문서 이용관련 분쟁 최소화
- 제 3자가 메시지를 가로채어 위장, 전자 서명한 것으로 오인
- 전자서명 검증키에는 소유자 정보가 포함되어 있지 않으며, 무결성 보장 않됨
- 전자서명 검증키와 소유자 정보를 하나의 문서로 만들어 상호 신뢰할 수 있는 제 3자를 통해 확인을 받는 방법이 제시

## 2. 주요 기반 기술

### 2.1 ACTIVE DIRECTORY

#### 2.1.1 ACTIVE DIRECTORY란 무엇인가

Active Directory는 Windows 2003 Server 네트워크의 디렉토리 서비스이다. 디렉토리 서비스란 네트워크 리소스에 대한 정보를 저장하여 사용자와 응용 프로그램이 리소스에 액세스 할 수 있게 만드는 네트워크 서비스이다. 디렉토리 서비스는 이러한 리소스에 대한 정보의 이름을 지정하여 설명을 제공하고 위치를 찾거나 액세스 및 관리, 보호하는 일관된 방법을 제공한다. Active Directory의 기능을 간략히 보면 다음과 같다.

##### 2.1.1.1 디렉토리 서비스 기능

Active Directory는 네트워크 리소스의 중앙 집중적 구성, 관리, 액세스제어 등 디렉토리 서비스 기능을 제공한다. Active Directory는 물리적 네트워크 토폴로지와 프로토콜을 투명하게 만들어 네트워크 사용자가 리소스의 위치나 물리적인 네트워크 연결 방법을 몰라도 액세스할 수 있게 한다. 이러한 리소스 유형의 예로는 프린터가 있다.

Active Directory는 섹션별로 구성되므로 수많은 개체를 저장할 수 있다. 결과적으로 Active Directory는 조직의 성장에 따라 확장이 가능하므로 단일 서버에서 수백개의 개체를 관리하는 조직이 수천대의 서버와 수백만개의 개체를 갖춘 조직으로 성장할 수 있다.

##### 2.1.1.2 중앙화된 관리

윈도우 2003을 실행하는 서버는 시스템 구성, 사용자 프로필, 응용 프로그램 정보를 Active Directory에 저장한다. 그룹 정책과 Active Directory를 함께 사용하면 관리자가 일관된 관리 인터페이스를 통하여 분산된 데스크톱, 네트워크 서비스, 응용 프로그램을 중앙에서 관리할 수 있다.

Active Directory는 또한 사용자가 단 한 번의 로그인을 통하여 Active Directory의 모든 리소스에 대한 전체 액세스 권한을 가질 수 있도록 네트워크 리소스에 대한 액세스를 중앙에서 제어할 수 있는 기능도 제공한다.

Active Directory는 스마트카드 배포를 구현하기 위한 핵심 요소이다. 윈도우 2003에서 제공되는 Active Directory는 기본적으로 스마트카드의 대화형 로그인 및 인증서에 대한 계정 매핑을 지원한다. 사용자 계정을 인증서에 매핑하는 이 기능은 스마트카드의 개인키를 Active Directory에 있는 인증서에 연결한다. 로그인 할 때 스마트카드 자격 증명을 제공하려면 Active Directory가 고유한 사용자 계정에 특정 카드를 일치시켜야 한다.

Active Directory는 또한 쉽게 스마트카드 로그인 과정 및 스마트카드 발급을 관리할 수

있도록 보안 그룹 및 그룹 정책을 지원한다.

#### 2.1.1.2-1 보안 그룹

Active Directory의 보안 그룹을 사용하여 사용자를 구성하면 매우 쉽게 스마트카드를 배포하고 관리할 수 있다. 예를 들어, 일반적인 스마트카드를 배포할 때는 다음과 같은 보안 그룹을 만들어야 한다.

스마트카드 등록 에이전트	스마트카드 등록 에이전트는 스마트카드를 사용자에게 배포하는 역할을 담당한다.
스마트카드 준비 그룹	스마트카드 준비 그룹에는 스마트카드를 받도록 승인되었지만 등록 에이전트에서 아직 해당 카드가 등록되지 않은 모든 사용자가 포함됩니다.
스마트카드 사용자 그룹	이 그룹에는 등록 과정이 완료되고 활성화된 스마트카드를 보유한 모든 사용자가 포함된다. 등록 에이전트는 스마트카드 준비 그룹의 사용자를 스마트카드 사용자 그룹으로 이동한다.
스마트카드 임시 예외그룹	이 그룹은 스마트카드를 분실했거나 잊고 가져오지 않은 경우 등으로 인해 스마트카드 요구사항에 일시적인 예외가 필요한 사용자를 위한 것이다.
스마트카드 영구 예외그룹	이 그룹은 서버에서 서비스나 예약된 작업을 실행하는 계정 또는 스마트카드 로그인 요구사항에 부합되지 않는 운영 체제 및 장치에서 작업하는 사용자 등과 같이 스마트카드 로그인을 위한 요구 사항에 영구적인 예외가 필요한 계정을 포함한다.

<표 2. 스마트카드 보안그룹>

#### 2.1.1.2-2 그룹 정책

그룹 정책을 사용하면 구성 설정을 여러 컴퓨터에 적용할 수 있다. 대화형 로그인에 스마트카드를 사용하기 위한 요구 사항을 그룹정책개체(GPO)에 설정한 다음 이 GPO를 Active Directory의 조직 구성단위나 사이트에 적용할 수 있다

### 2.1.2 ACTIVE DIRECTORY의 구조

AD는 계층 구조를 띄고 있다. AD를 인스톨하기 전에 사용자는 AD의 구조와 각 컴퍼넌트들에 대해서 잘 이해하고 있어야 효율적인 AD 디자인을 할 수 있다.

또한, Active Directory는 논리적 구조와 물리적 구조로 나뉘어진다. 논리적 구조에는 도메인(Domain), 트리(Tree), 포리스트(Forest), OU(Organizational Unit) 등이 있으며, 물리적 구조에는 도메인 컨트롤러(Domain Controller), 글로벌 카탈로그 서버(Global Catalog Server), 사이트(Site) 등이 있다.

#### 2.1.2.1 논리적 구조

##### - Object (오브젝트)

AD에서의 오브젝트란 네트워크상에 위치한 물리적 아이템(Physical Object)를 뜻한다. AD 오브젝트로는 사용자, 그룹, 프린터, 공유 폴더, 애플리케이션, 데이터베이스 등등이 될 수 있다. 각 오브젝트는 사용자가 확인 가능한 유형물이며, 각 오브젝트는 속성(Attributes)

을 갖고 있다. 예를 들면, 사용자 오브젝트(User Object)는 사용자 계정(Username), 실제 이름(Actual name), 전자 메일 주소와 같은 속성을 지닌다. 오브젝트의 종류에 따라 속성이 다르며, AD에 의해 정의된다. 이 속성을 통해 오브젝트를 특성화 할 수 있으며 사용자가 오브젝트를 찾는데 도우미 역할을 할 수 있다.

#### - Organizational Unit (이하 OU)

OU는 파일 캐비닛의 파일 폴더와 같은 것이다. OU는 오브젝트를 담기 위해 디자인된 그릇으로 보면 된다. 또한 OU가 OU 자체를 담을 수도 있다. OU는 오브젝트를 담는 역할만 하지 자체적으로 어떠한 기능을 하진 않는다. 파일 폴더로서 OU는 오브젝트를 담는데 그 목적이 있는 것이다. 이름에 나타난 바와 같이 OU는 사용자 하위 디렉토리 구조를 조직화 하는데 도움을 준다. 예를 들면, 사용자는 Accounting이라고 불리는 OU를 만들어 Accounting Group A OU와 Accounting Group B OU를 담을 수 있다. 물론 A/B OU에는 자신들만의 사용자, 컴퓨터, 프린터 등등의 오브젝트를 담고 있을 수 있다. OU는 또한 보안과 관리의 경계선으로도 사용될 수 있고 다중 윈도우 NT 도메인 네트워크안의 도메인을 교체하는데 사용될 수 있다.

#### - Domain (도메인)

간단하게 정의하면 도메인이란 사용자와 컴퓨터를 논리적으로 그룹화 시킨 영역을 말한다. 모든 각 도메인은 자신만의 Security Policies를 갖고 있으며, 다른 도메인과 Trust 관계를 맺을 수 있다. AD는 하나 이상의 도메인으로 구성되며, 스키마(Schema : a set of object class instances)를 포함하고 있다. 스키마가 하는 역할은 특정 오브젝트가 AD내에서 어떻게 규정되어 있는가를 결정하는 기준점이 된다. 이 스키마는 AD내에 존재하며, 계속적으로 변이된다.

#### - Tree (트리)

도메인, OUs, 오브젝트의 계층적 구조를 트리(Tree)라 부른다.

#### - Domain Trees (도메인 트리)

도메인 트리는 트러스트 관계를 맺고 있고 스키마, 설정(configuration), 글로벌 카탈로그를 공유하고 있을 때 나타나게 된다. 윈도우 2003에서 트러스트 관계(Trust Relationships)는 Kerberos Security Protocol을 사용한다. Kerberos trusts는 transitive 한데, 이 말은 도메인 1이 도메인 2를 트러스트하고 도메인 2가 도메인 3을 트러스트 하면, 도메인 1도 도메인 3을 트러스트 한다는 의미다.

#### - Fores (포레스트)

포레스트는 서로 다른 contiguous namespace를 갖고 있는 하나 이상의 도메인이 모여 만들어진 구조를 갖고 있다. 예를 들면, microsoft.com 도메인과 nortelnetworks.com 도메인은 서로 다른 contiguous namespace를 갖고 있다. microsoft.com이 nortelnetworks.com을 합병시켰고, 이 두 도메인이 서로 트러스트해야 될 경우가 생겼다면, 포레스트로 이 두 도메인을 트러스트 시켜 정보를 공유할 수 있게 할 수 있다. 포레스트 트러스트로 묶여 있는 각 도메인의 트러스트 관계는 transitive trust다.

### 2.1.2.2 물리적 구조

#### - Domain Controller (도메인 컨트롤러)

도메인 컨트롤러란 디렉토리 복제를 저장하는 Windows 2003 Server 컴퓨터이다. 도메인 컨트롤러는 또한 디렉토리 정보의 변경 내용을 관리하고 이러한 변경 내용을 같은 도메인에 있는 다른 도메인 컨트롤러로 복제한다. 도메인 컨트롤러는 디렉터리 데이터를 저장하고, 사용자 로그인 프로세스를 관리하고, 인증하고, 디렉터리 검색을 제공한다.

한 도메인은 하나 이상의 도메인 컨트롤러를 가질 수 있다. 하나의 LAN을 사용하는 작은 조직에서는 두 개의 도메인 컨트롤러와 하나의 도메인만으로 충분한 가용성과 내결함성을 제공한다. 그러나 지역적으로 여러 위치로 분산된 대규모 조직에서는 각 위치마다 하나 이상의 도메인 컨트롤러가 있어야 충분한 가용성과 내결함성을 제공할 수 있다.

#### - Site (사이트)

사이트는 AD 계층적 구조와는 상관이 없는 개념이다. 하지만 AD Replication의 목적으로 사용되는 수단으로서 설정되어 사용된다. 사이트는 TCP/IP 서브넷으로 잘 연결되어 있는 AD 서버를 갖고 있는 네트워크를 지리적으로 묶을 때 유용한 기술이다. 여기서 잘 연결되어 있다라고 함은 각 AD 사이의 네트워크 연결이 아주 안정적으로 운영되어 있어 통신에 있어 문제가 일어나지 않는다는 것을 의미한다. 관리자는 연결된 Sites를 통해 AD Replication을 서로 복제 시킨다.

#### -글로벌 카탈로그 서버 (Global Catalog Server)

글로벌 카탈로그란 Active Directory의 모든 개체 특성의 일부를 포함하는 정보 저장소이다. 기본적으로 글로벌 카탈로그에 저장되는 특성은 사용자의 이름, 성, 로그인 이름 등과 같은 쿼리에서 가장 자주 사용되는 요소들이다. 글로벌 카탈로그에는 디렉터리에서의 개체 위치를 판단할 수 있는 정보가 저장된다.

## 2.2 SMART CARD

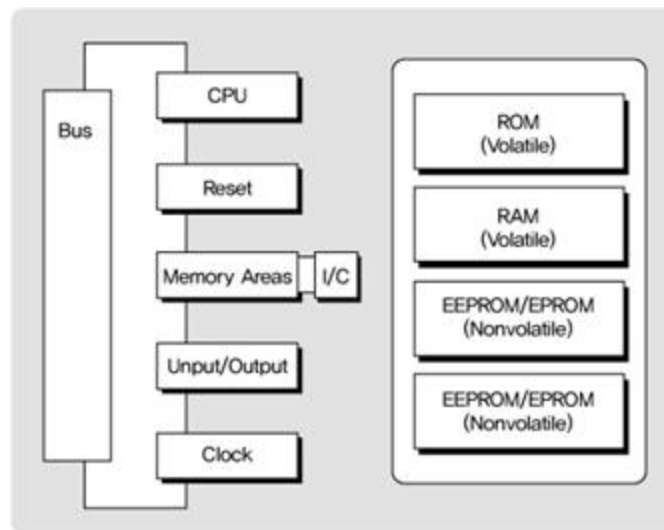
### 2.2.1 SMART CARD란 무엇인가

플라스틱 재질의 신용 카드 크기인 스마트카드에는 마이크로컴퓨터와 작은 용량의 메모리가 수록되어 있어 개인키와 X.509 보안 인증서를 안전하고 위조할 수 없게 저장한다. 스마트카드는 일반적으로 단지 1KB의 RAM과 함께 32KB 또는 64KB의 EEPROM(Electrically Erasable Programmable Read Only Memory) 및 ROM(Read Only Memory)을 포함하고 있다. ROM에는 스마트카드 운영 체제가 수록되어 있으며 EEPROM에는 파일 및 디렉터리 구조, PIN 관리 애플릿 및 인증서가 수록되어 있다. RAM은 암호화와 암호 해독과 같은 카드 작업을 위한 작업 메모리를 제공한다.

### 2.2.2 SMART CARD의 내부 구조

스마트카드는 8비트, 16비트 또는 32비트 CPU를 보유한 소형 컴퓨터의 기능을 가지고 있다. 온칩(On-Chip) 메모리는 재 프로그램이 가능하고, 그 분야에서 스마트카드의 탄력성에 영향을 주고, 하나의 카드로 하나 이상의 어플리케이션에 사용되도록 설계되는 기회를 제공한다.

카드는 저장매체로서의 기능뿐만 아니라 키패어의 개발, 디지털 서명의 인증, 데이터 보호 역할을 하는 컴퓨터의 역할도 수행한다 할 수 있다. 일반적인 스마트카드의 내부는 다음의 그림과 같다.



<그림 1. 스마트 칩의 내부>

### 2.2.3 SMART CARD 사용의 기대 효과

스마트카드와 연결된 PIN 방식은 이중 인증 중에서도 많이 사용되고, 안정적이고, 비용 효율적인 형태이다. 적절하게 관리한다면, 스마트카드를 가지고 있고 암호를 아는 사용자만 네트워크 리소스 액세스 권한을 획득할 수 있다. 이중 요구 사항은 조직의 네트워크에 대한 무단 액세스 가능성을 현저하게 감소시킨다.

스마트카드는 다음과 같은 두 가지 시나리오에서 특히 효과적인 보안 제어를 제공한다. 관리자 계정 보안 및 원격 액세스 보안이 그것이다.

관리자 수준의 계정은 넓은 범위의 사용자 권한을 보유하기 때문에, 이러한 계정 중 하나라도 노출될 경우 전체 네트워크 리소스에 침입자가 액세스할 수 있는 권한을 부여한다. 도메인 관리자 수준의 계정 자격 증명이 도난되면 도메인 전체를 위협에 빠트리고, 심지어 전체 포리스트 또는 다른 신뢰할 수 있는 포리스트까지도 영향을 받을 수 있기 때문에, 관리자 수준 액세스 권한을 안전하게 보호하는 것은 매우 중요하다. 관리자 인증에 대해 이중 인증 방식의 사용은 필수적이다.



조직은 네트워크 리소스에 원격 연결이 필요한 사용자에게 스마트 카드를 배포할 경우, 중요한 추가 보안 계층을 제공할 수 있다. 원격 사용자에게도 이중 인증은 특히 중요한데, 이는 원격 연결에 대해 어떠한 형태의 물리적 액세스 제어도 제공하는 것이 불가능하기 때문이다. 스마트카드를 사용한 이중 인증은 VPN(가상 사설망) 연결을 통해 연결하는 원격 사용자의 인증 프로세스 보안을 강화할 수 있다.

## 2.3 USB TOKEN

### 2.3.1 USB TOKEN이란 무엇인가

USB토큰이란 한마디로 스마트카드 칩을 내장한 USB장치로, 1980년대 초 프랑스에서 도입한 이후로 현재까지 어떠한 물리적, 논리적 해킹도 성공하지 못한 최고로 안전한 인증장치이다.

국내에는 물론 국제 표준규격의 공인 인증서 저장 매체로서 금융권 / 사설 공인 인증의 목적으로 널리 사용되고 있는 저장 장치 이다. 온라인상의 인감도장이라 불리울 만큼 사용 및 휴대가 편리하고 하드디스크, 플로피디스크, USB 메모리 등의 매체와는 달리 저장된 인증서 파일을 Windows 탐색기 등에서 확인이 불가능하여 해킹이나 바이러스 등으로부터 안전하다. USB토큰은 암호토큰의 역할이 가능한 스마트카드와는 달리 누구나 쉽고 편리하게 사용할 수 있도록 USB장치 형태로 만들어져, 휴대가 간편한 암호토큰이다.

또한, USB장치이기 때문에 실제 리더기 대신 소프트웨어 형태의 리더기를 이용하여 한번 설치 후 USB포트를 이용해 리더기가 따로 필요 없다.

### 2.3.2 USB TOKEN의 효과

암호토큰(HSM, Hardware Security Module)'으로 불리는 인증용 USB는 각종 PC해킹으로 인한 정보유출을 막을 수 있어 전자상거래 시대에 강력한 보안 수단으로 떠오르고 있다. 일반 시중에서 판매하는 USB는 보안 기능을 갖추고 있지 않은 단순한 하드디스크 메모리이기 때문에 PC CPU로 연산하는 과정에서 해킹으로 인한 정보유출 우려가 있다.

하지만 USB 형태의 암호토큰은 저장장치 안에서 키 생성과 전자서명이 이뤄지기 때문에 인증키가 외부로 유출되지 않아 인증서를 안전하게 보관할 수 있다. 또한 인증서를 하드디스크에 저장하는 방식이 아닌 스마트카드와 같은 외부장치로 인증하는 방식이라 더욱 안전하다.

### 3. 인증 시스템의 필요 기술

#### 3.1 ACTIVE DIRECTORY

앞에서도 말했듯이 Active Directory는 스마트카드 배포를 구현하기 위한 핵심 요소이다. 스마트카드로의 로그인 및 스마트카드 발급을 관리함에 있어 보안 그룹과 그룹정책 등을 지원한다.

#### 3.2 SMART CARD 및 USB TOKEN (물리적 인증 도구)

스마트카드와 USB토큰으로의 인증을 함에 있어 스마트카드 리더기와 스마트카드, USB토큰 등이 필요하다.

#### 3.3 시스템 환경

##### 3.3.1 환경 구축을 위한 구성 요소

SMART CARD 및 USB TOKEN 운영 체제 및 네트워크 요소에서 지원되는 적절한 인프라가 필요하다. Microsoft는 스마트카드 구현을 위해 다음과 같은 구성 요소를 지원한다.

- Microsoft 인증서 서비스 또는 외부 공개키 구조(PKI)
- 인증서 템플릿
- Windows Server 2003
- Active Directory 디렉토리 서비스  
(보안그룹, 그룹정책, 등록 스테이션 및 등록 에이전트, 활성화 웹 서버)
- EAP-TLS (확장할 수 있는 인증 프로토콜-전송 계층 보안) :원격 액세스 솔루션에 필요  
추가구성 요소에는 등록 스테이션과 등록 에이전트가 포함된다.

다음으로 클라이언트 및 서버의 사양과 필요 기술을 다음과 같이 서술할 수 있다.

COMPUTER		SERVER SOFTWARE	CLIENT SOFTWARE
CPU	Pentium 4 2.6GHz	Windows Server 2003 Enterprise Edition	Windows XP Professional
RAM	1GB	GemPlus Smart Card Reader Driver	GemPlus Smart Card Reader Driver
Graphic Card	GeForce 2	Shin Wha SH-CSP 2.6	Shin Wha SH-CSP 2.6
HDD	60GB	USB Token	USB Token
LAN Card	3 Com		
GemPlus, GemPC 410			
Smart Card, USB Token			

<표 3. 시스템 구축 사양 및 필요기술>

### 3.3.2 환경 구축을 위한 시스템 기반 구조

#### - 구현 전제 조건

스마트카드를 배포하려면 조직에서 구현 단계를 시작하기 전에 모든 문제점을 고려할 수 있도록 체계적인 접근 방식이 요구된다. 여기서는 가장 일반적인 전제 조건을 다루지만 사용자의 환경에 따라 추가적인 요구 사항이 있을 수 있다.

#### - 계정 인증

스마트카드를 배포함에 있어 스마트카드를 사용하여 액세스해야 하는 사용자 및 그룹을 파악하는 과정은 중요한 부분이다.

또한 이사회 중역과 같이 위의 목록에 없는 사용자 및 그룹도 스마트카드 액세스가 필요할 수 있다. 이러한 계정을 구현 과정 초기에 파악하면 프로젝트 및 제어 비용의 범위를 파악하는 데 도움이 된다.

중요한 계정을 파악하려면 언제 스마트카드를 사용할지를 결정해야 한다. 예를 들어, 관리자는 전자 메일과 같은 일상 작업 처리를 위한 표준 계정과 서버 관리 및 기타 관리 작업 처리를 위한 관리자 수준 계정의 두 개의 사용자 계정을 사용하는 것이 보안상 바람직하다.

대개 관리자는 사용자 수준 계정을 사용하여 로그인하고 Secondary Logon 서비스를 사용하여 관리 작업을 수행한다. 또는 스마트카드 로그인을 지원하는 Windows Server 2003의 관리용 원격 데스크톱 구성 요소를 사용할 수도 있다.

#### - 스마트카드 인프라 지원

스마트카드는 운영 체제 및 네트워크 요소에서 지원되는 적절한 인프라가 필요하다.

#### - PKI(공개 키 구조)

스마트카드를 사용하려면 Active Directory에서 계정 매핑이 가능하도록 PKI에서 공개 키/개인 키 쌍을 가진 인증서를 제공해야 한다. 이 PKI는 외부 조직에 내부 인증서 구조를 제공하거나 Windows Server 2003의 인증서를 사용하는 두 가지 방법 중 하나로 구현할 수 있다. 조직은 스마트카드를 위한 인증서 관리 과정의 전체 또는 일부를 아웃소싱 할 수 있다.

재무 조직의 경우 전자 메일 확인 및 파트너와 보안 트랜잭션을 위해 PKI를 외부의 신뢰

할 수 있는 루트로 링크하면 유용하다. 다른 방법은 Windows Server 2003의 인증서 서비스를 사용하여 PKI를 제공하는 것이다.

PKI에는 인증서 해지를 처리하는 메커니즘이 있어야 한다. 인증서 해지는 인증서가 만료되거나 공격자에 노출된 경우 필요하다. 각 인증서는 인증서 해지 목록(CRL)의 위치를 포함하고 있다.

#### **- 인증서 템플릿**

Windows Server 2003에는 스마트카드에서 사용하는 디지털 인증서를 발급하는 특정 인증서 템플릿이 포함되어 있다. 이러한 인증서를 복사한 다음 조직의 요구 사항에 맞게 사용자 지정할 수 있다.

Windows Server 2003 Enterprise Edition은 로그인, 서명된 전자 메일 메시지 및 파일 암호화와 같은 여러 기능을 제공하도록 수정하고 확장할 수 있는 버전 2(v2) 템플릿을 제공한다. 또한 건강 검진 자료나 연금 내역과 같이 조직에 필요한 추가 정보를 제공하도록 인증서 템플릿을 확장할 수도 있다. Windows Server 2003 Enterprise Edition은 대규모 조직에서 스마트카드를 보다 쉽게 관리할 수 있는 자동 등록을 지원한다. 인증서 갱신 요청을 받으면 현재 인증서를 사용하여 요청에 서명할 수 있다.

#### **- Windows Server 2003**

Microsoft Windows 2000 Server는 콘솔 로그인 전용의 관리자 인증 및 원격 액세스를 위한 스마트카드를 지원한다. 관리자를 위한 스마트카드를 구현하려면 관리되는 서버가 RDP(원격 데스크톱 프로토콜) 연결을 통한 스마트카드 로그인과 같은 보조 작업을 지원하는 Windows Server 2003을 실행해야 한다. 이 운영 체제 요구 사항에는 도메인 컨트롤러도 포함된다.

#### **- Active Directory**

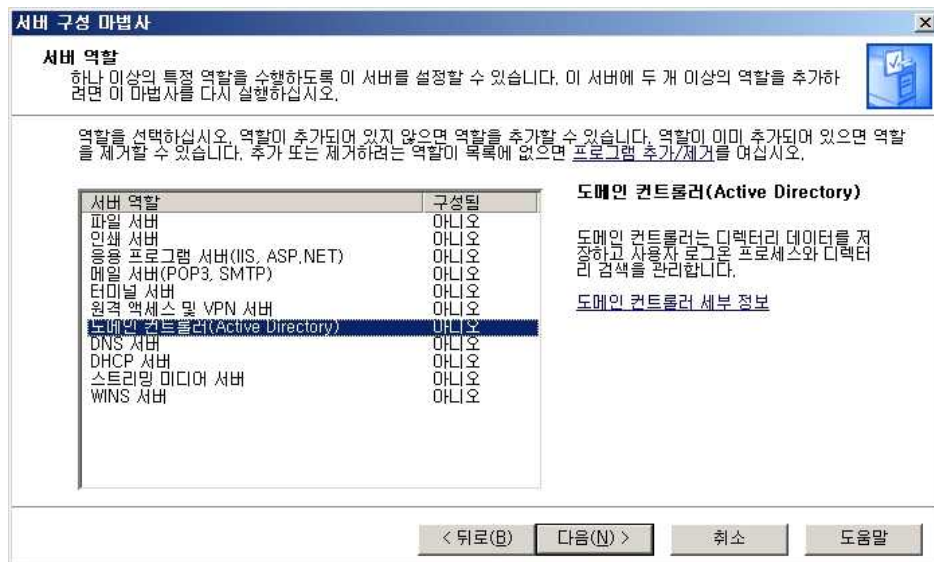
스마트카드 로그인 과정 및 스마트카드의 발급 등을 관리하기 위한 핵심 요소이다.

## 4. 인증 시스템의 기술적 구현 및 사용 방법

### 4.1 ACTIVE DIRECTORY의 구현

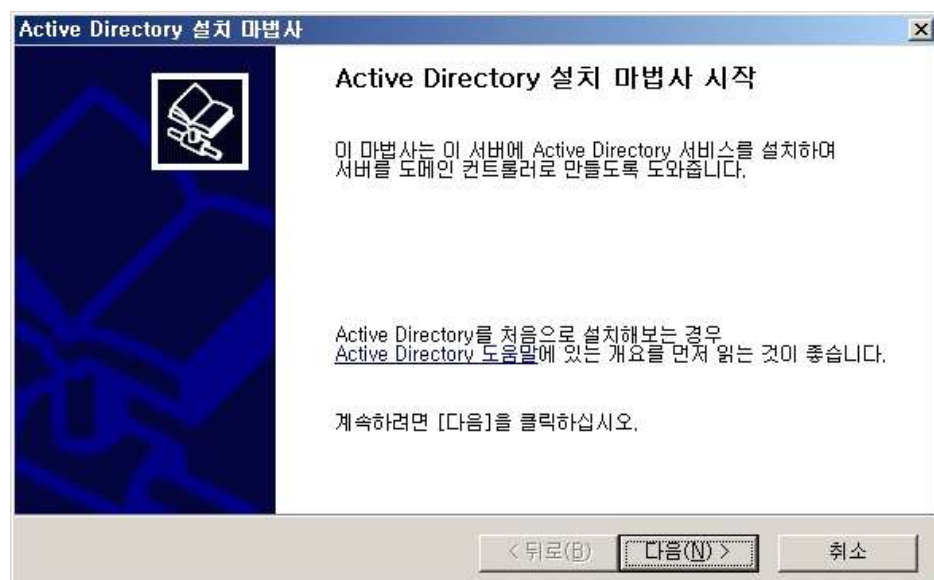
#### 4.1.1 ACTIVE DIRECTORY 설치

- 먼저 시작메뉴-실행 창을 열고 "dcpromo.exe"를 실행 한다 확인을 눌러 Active Directory 설치 마법사를 시작하고 새 도메인의 도메인 컨트롤러를 누르고 다음을 누른다.



<그림 2. AD 설치준비>

- 마법사를 실행하면 몇 가지 옵션을 결정하고 입력해 주어야 하는데 복수도메인 환경을 셋팅 하기 위해서는 잘 이해해야 할 옵션이다.



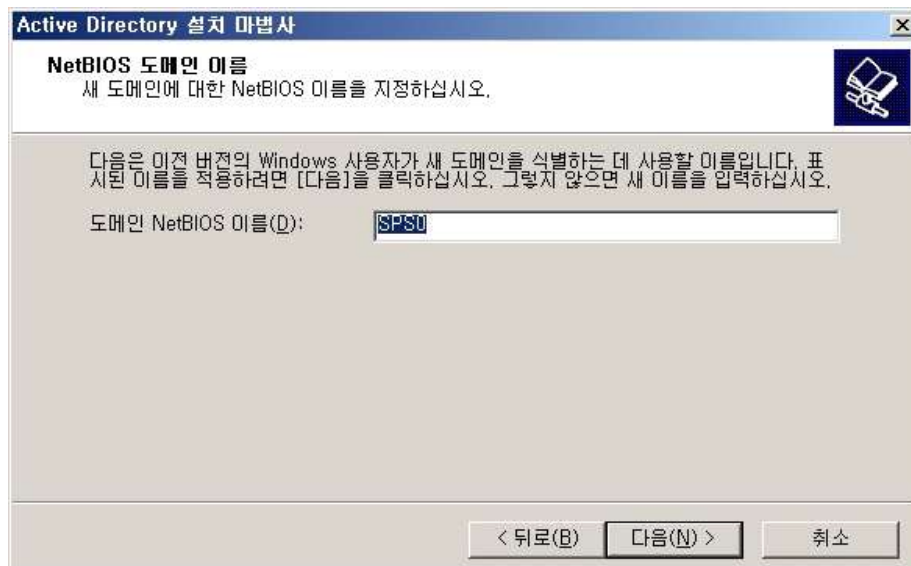
<그림 3. AD 설치>

- DNS도메인 이름을 정한다. 우리는 여기서 조이름을 이용하여 SPs.com을 사용하였다.



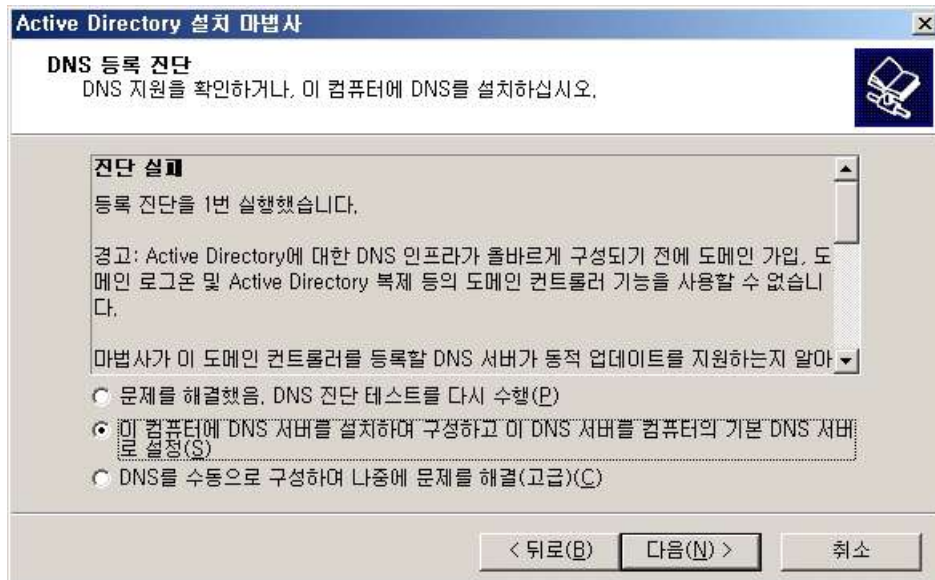
<그림 4. 도메인 지정>

- 도메인 NetBIOS이름을 정해준다



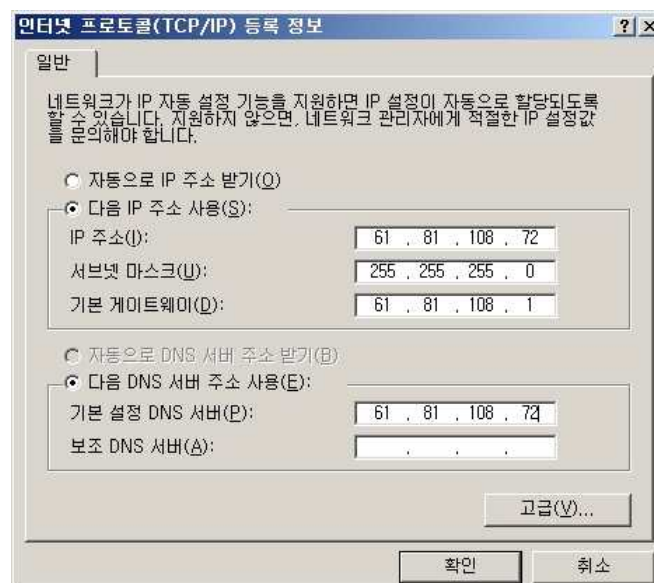
<그림 5. NetBIOS 도메인명 지정>

- DNS등록 진단을 처음 실행하면 볼수 있는 오류 화면이다 이화면의 오류는 지금 서버에 DNS서버가 구축되어 있지 않다는 내용이다 처음 설치하는 서버이므로 DNS서버를 설치하는 옵션을 선택한다.



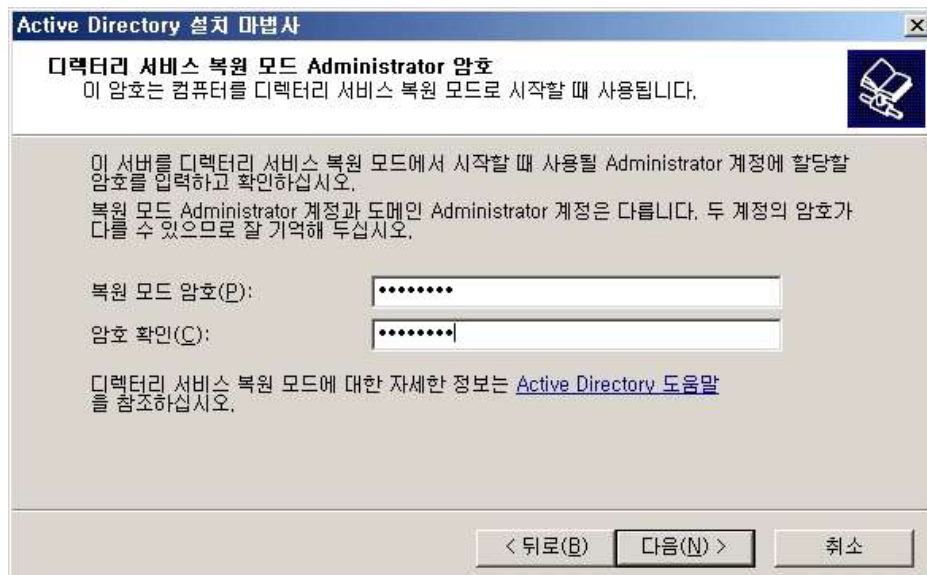
<그림 6. DNS등록 진단>

- DNS서버를 이용하기 위하여 고정 IP를 잡아준다



<그림 7. IP 설정>

- 복원모드 PASSWORD를 입력하고 다음을 누르면 옵션선택내용이 나온다 옵션 선택내용을 확인하고 다음을 클릭한다.

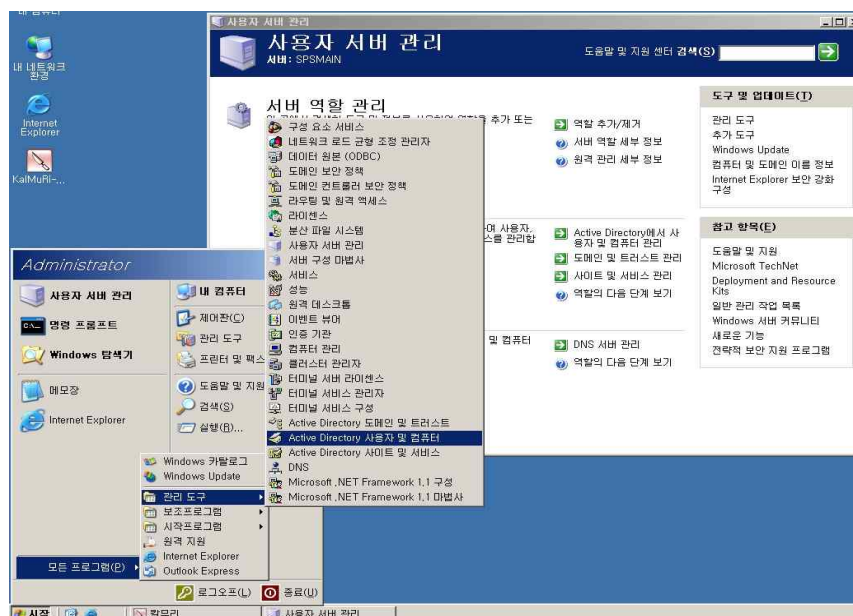


<그림 8. 복원모드 암호설정>

- 컴퓨터를 다시 시작할 것인지 물으면 예를 누른다. 컴퓨터가 다시 시작되면 새로운 도메인 컨트롤러에 대한 DNS(Domain Name System) 서비스 위치 레코드가 만들어져 있다. DNS 서비스 위치 레코드가 만들어졌는지 확인한다.

#### 4.1.2 엔터프라이즈 관리자 계정 변환

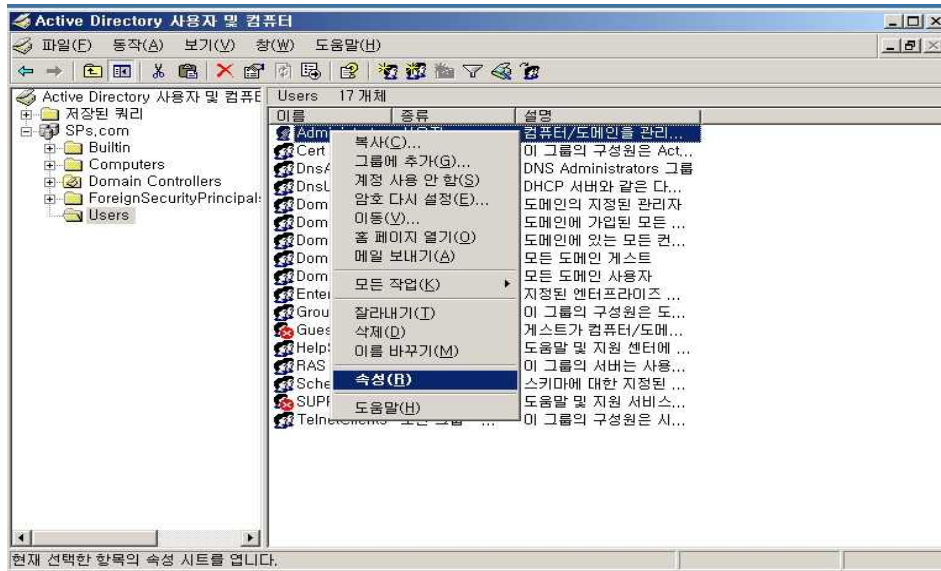
- AD 사용자 및 컴퓨터를 선택 한다.



<그림 9. AD사용자 및 컴퓨터>

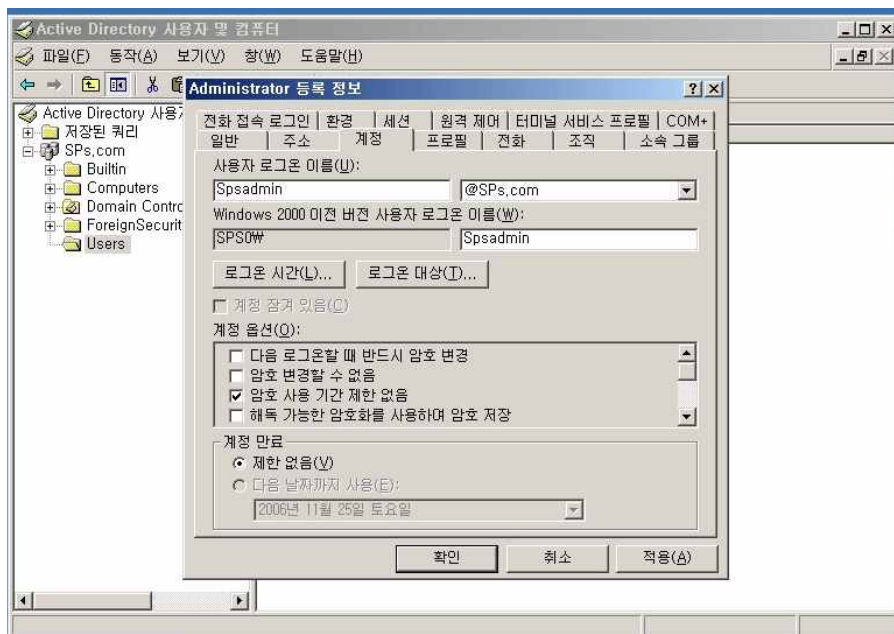


- Admin 계정에서 속성 탭을 선택한다.



<그림 10. 관리자 속성>

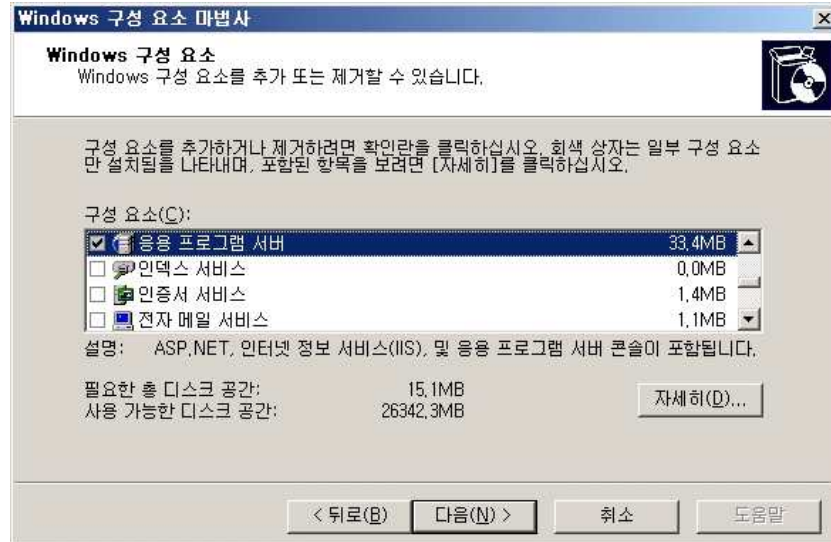
- 계정명을 SPsadmin으로 설정하고 도메인을 SPs.com으로 설정하여준다



<그림 11. AD 관리자 세부설정>

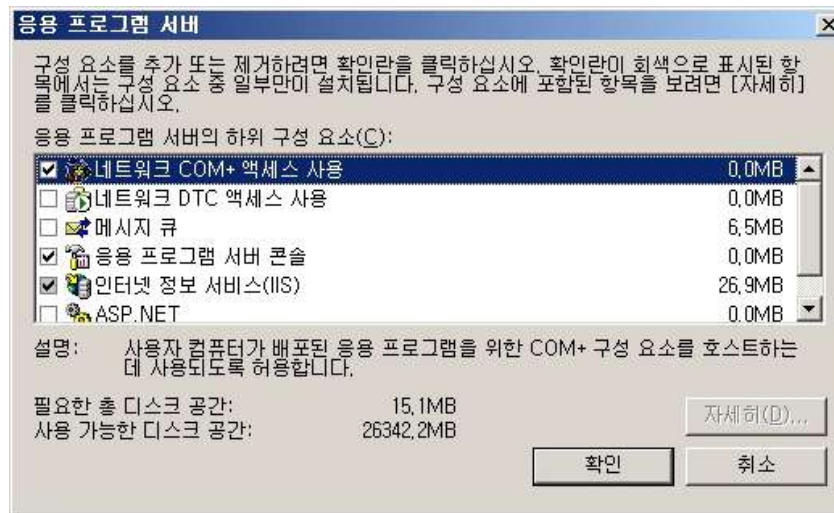
### 4.1.3 IIS 설정

- 응용 프로그램 서버를 선택하고 다음을 누른다.



<그림 12. IIS 서비스 설정>

- 다음으로 구성요소를 선택한 뒤 확인을 누른다.



<그림 13. IIS서비스 속성 선택>

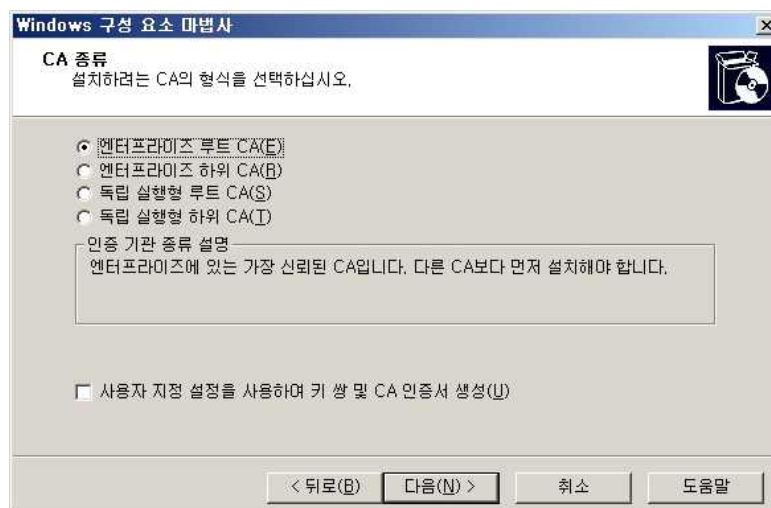
- 다음과 같이 구성 요소 마법사가 완료되면 마침을 누른다.



<그림 14. IIS 서비스 구성 완료>

#### 4.1.4 엔터프라이즈 루트 CA 설치

- 인증서 설치를 선택하고 엔터프라이즈 루트 CA를 선택 한다  
(AD가 설치되어 있지 않으면 엔터프라이즈 루트 CA를 선택할 수 없다.)



<그림 15. 엔터프라이즈 루트 CA 설치>



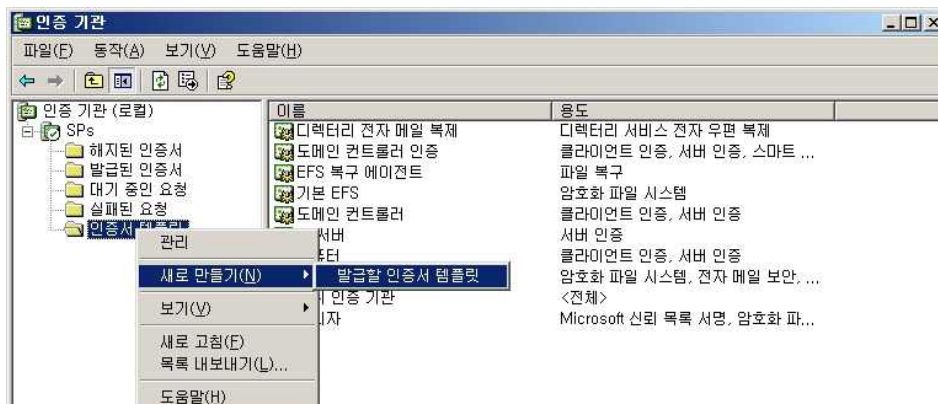
<그림 16. CA 설치 알림 창>

- 인증 데이터베이스를 설정하고 다음을 누른다.



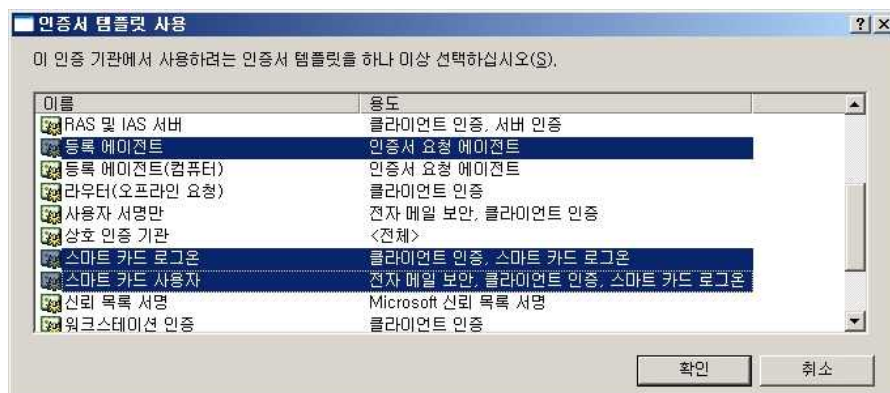
<그림 17. 인증서 DB 설정>

- 인증기관이 설치되면 인증서 템플릿을 선택 한다



<그림 18. 인증서 템플릿 추가>

- 인증서 템플릿에서 등록 에이전트와 스마트카드 로그인 사용자 템플릿을 선택한다.

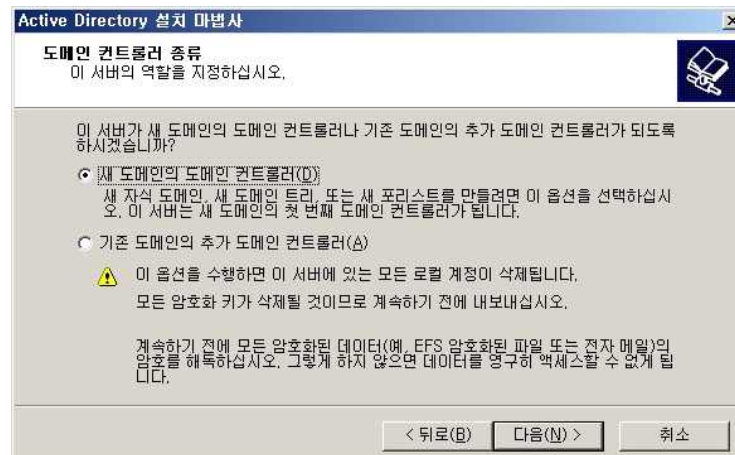


<그림 19. 사용할 인증서 템플릿 선택>



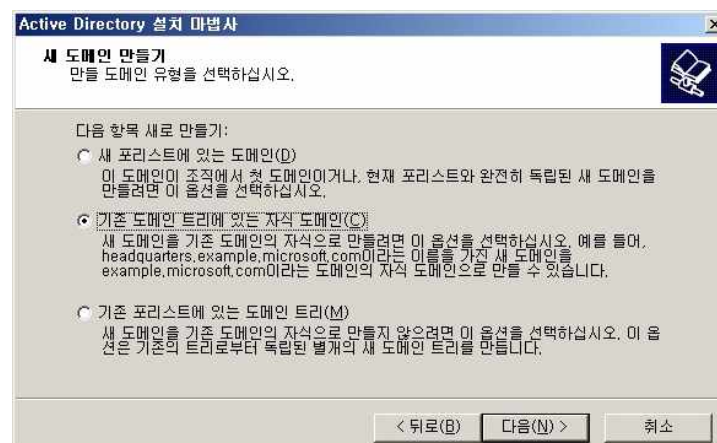
<그림 20. 추가된 인증서 템플릿>

- 기존 도메인 컨트롤러와 연동할 ‘자식 도메인컨트롤러’ 설치를 하기 위해 AD설치 마법사를 실행하고 새 도메인의 도메인 컨트롤러를 선택한다.



<그림 21. 새 도메인 컨트롤러 선택>

- 기존 도메인인 SPs의 자식도메인을 만들 것 이므로 두 번째 옵션을 선택하여 준다.



<그림 22. 자식 도메인 선택>

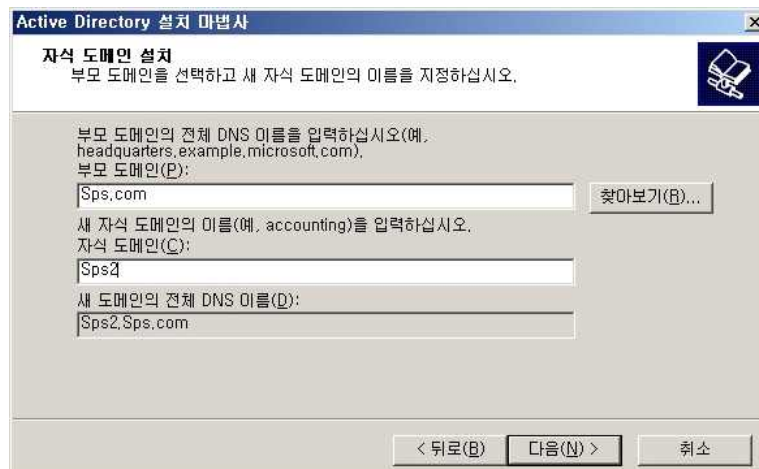


- 추가될 도메인 컨트롤러 사용자의 이름과 계정암호, 도메인명을 입력한다.



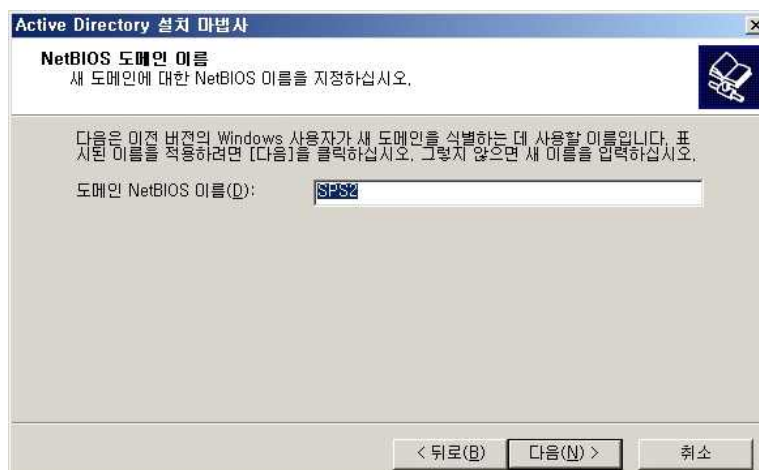
<그림 23. 도메인 컨트롤러 사용자 설정>

- 부모 도메인과 자식도메인의 이름을 정하여준다.



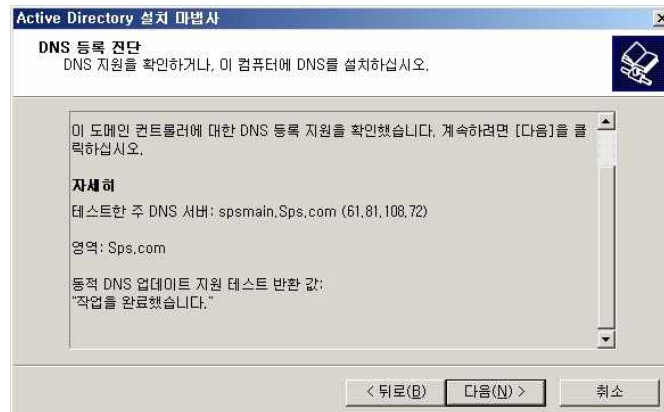
<그림 24. 도메인명 설정>

- 도메인 NetBIOS를 선택하여 준다.



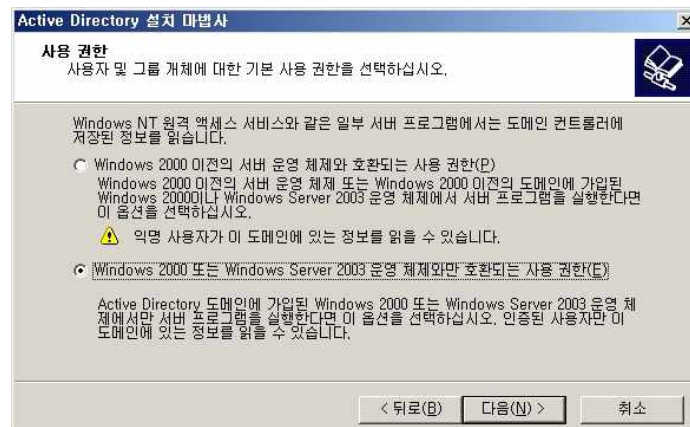
<그림 25. NetBIOS 이름 선택>

- 하위 등록기관에서 인증서를 발급 권한을 부여할 계정을 선택하고 DNS 등록 진단 내용을 확인한다. 여기서 메인서버 DNS를 설정하여 줄때동적 업데이트 옵션을 '보안되지 않은 동적업데이트 허용'을 사용하여 주어야 DNS설정이 오류 없이 진행된다.



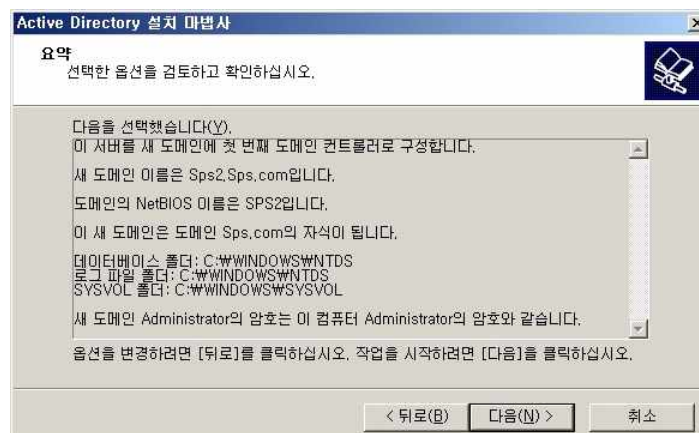
<그림 26. DNS 등록 진단>

- Windows 2000 또는 2003운영체제와 호환되는 사용권한을 선택



<그림 27. 사용 권한설정>

- 설정되어진 옵션들을 모두 확인하고 다음을 클릭한다.



<그림 28. 옵션 확인>

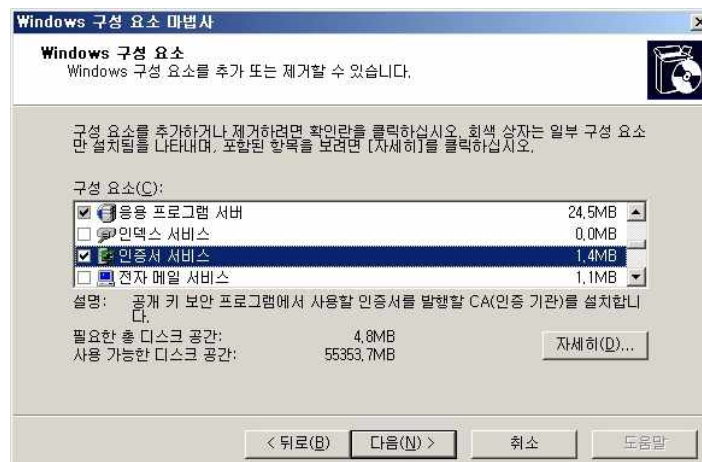
- 마침 버튼을 누르면 재부팅 확인창이 뜨고 확인을 누르면 재부팅이 실시된다.



<그림 29. AD설치 완료>

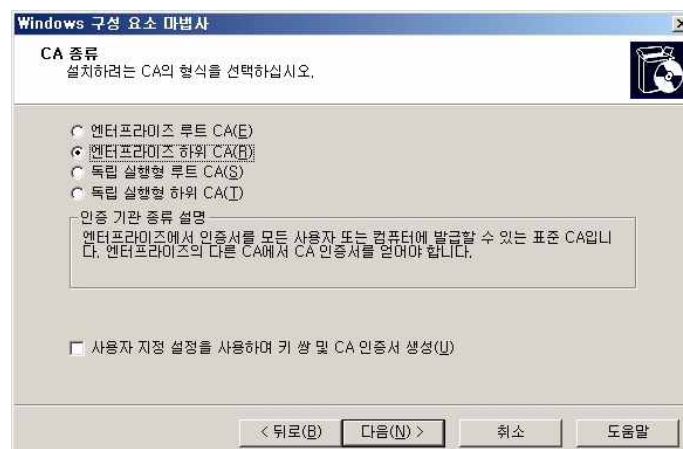
#### 4.1.5 하위 CA 설치

- 상위 CA를 설치했던 방식처럼 IIS를 설치한다. 인증서 서비스 선택하면.



<그림 30. CA설치>

- 엔터프라이즈 하위 CA를 선택한다.



<그림 31. 하위 CA>

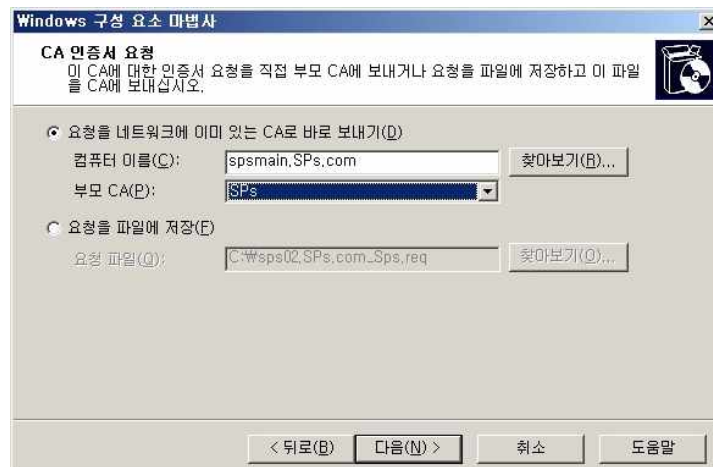


- 하위 인증센터의 CA 이름을 선택하여 준다.



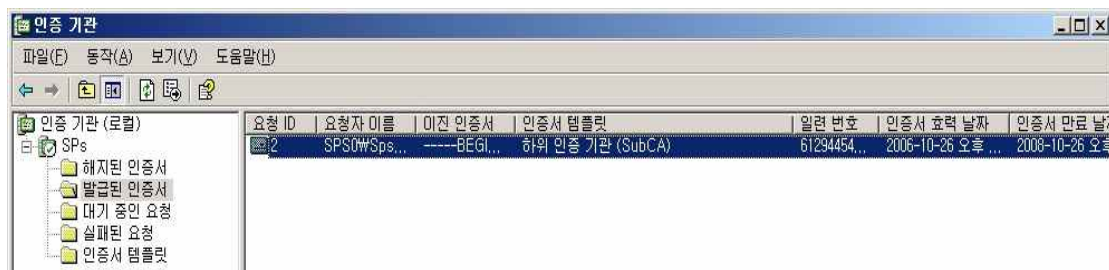
<그림 32. 하위 CA 이름입력>

- 상위 CA의 인증을 받기위한 정보를 입력하여 준다. 상위 CA를 선택하여 주면 CA에서 인증을 처리 하여 준다.



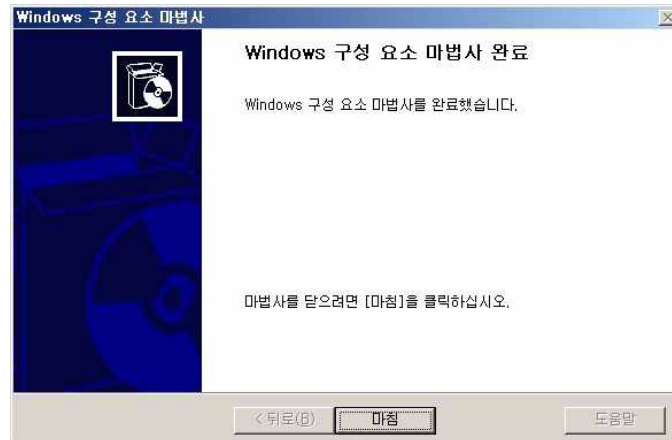
<그림 33. 하위 CA 인증서 요청>

- 위의 그림은 상위 CA에서 하위인증기관을 인증하여준 인증서의 모습이다.



<그림 34. 인증서 발급확인>

- 인증CA 설치 완료 화면.



<그림 35. CA 설치 완료>

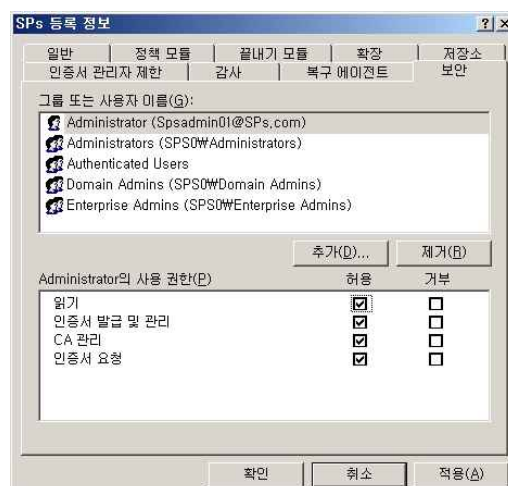
#### 4.1.5-1 하위 인증CA 권한부여

- 하위 인증센터에서 인증서를 발급하여 줄 수 있는 관리자에게 상위 서버에서 권한을 부여하는 모습이다.



<그림 36. 권한부여>

- 인증서관리 및 인증서를 요청할 수 있는 권한을 부여한다.



<그림 37. 상세 권한 설정>

## 4.2. SMART CARD의 구현

### 4.2.1 SMART CARD 시스템의 구현 단계 및 시스템 통합 과정

설치에 앞서 스마트카드 시스템을 구현 하는데 필요한 단계를 간단히 보면 다음과 같다.

- 스마트카드를 사용하는 계정을 통해 대화형 로그인, 보조 로그인, 원격 데스크톱 로그인을 지원하도록 대상 서버를 구현한다.
- 스마트카드를 사용하는 도메인 수준의 관리자 계정이 필요한 관리자를 파악한다.
- 스마트카드 판독기를 배포 한다
- 스마트카드를 배포하고 관리자를 등록하는 보안 프로세스를 개발한다.

그리고 다음 목록은 원격 액세스를 위해 스마트카드 시스템을 통합하는 데 필요한 과정을 개괄적으로 설명한다.

- 스마트카드 인증을 지원하도록 원격 액세스 서버를 업그레이드한다.
- 원격 액세스에 스마트카드를 사용해야 하는 사용자를 파악한다.
- 스마트카드 판독기를 배포한다.
- 스마트카드를 적절한 관리자에 배포하고 원격 사용자를 등록한다.

### 4.2.2 SMART CARD 설치

#### 4.2.2-1 스마트카드를 사용한 관리자 계정 보호

Windows Server 2003은 보조 작업에 대한 스마트카드 인증을 지원하여 사용자와 관리자 계정을 보다 효과적으로 격리할 수 있다. 일상적인 작업은 관리자가 비관리 계정으로 워크스테이션에 로그인 하여 수행할 수 있다. 관리 작업을 수행해야 하는 경우 관리자는 스마트카드를 사용하여 보조 작업을 인증할 수 있다. 이는 관리자가 사용자 이름과 암호를 입력해야 하거나 로그오프 한 다음 관리자 계정으로 다시 로그인 하는 것 보다 안전하고 편리한 방법이다.

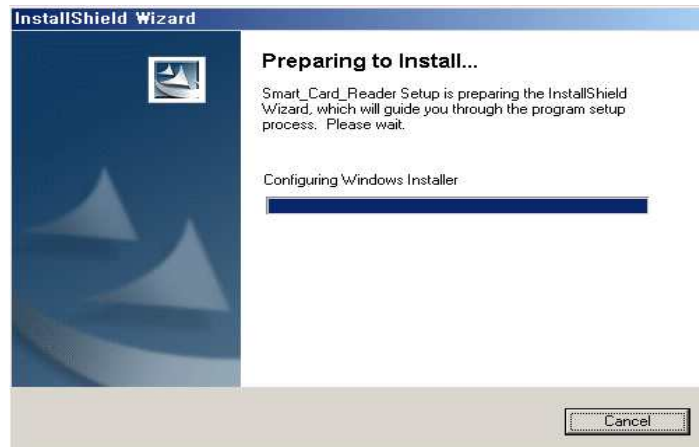
### 4.2.3 CSP(Cryptographic Service Provider) 설치 절차와 방법

설치에 앞서 CSP(암호화 서비스 공급자)에 대하여 간략하게 본다면 CSP는 Windows 운영 체제에서 일반 암호화 기능을 제공 하는 하드웨어 및 소프트웨어 구성요소이다. Windows Server 2003 제품군에는 여러 CSP가 포함되어 있으며, 사용자가 다른 CSP를 추가설치 할 수도 있다. 이러한 CSP는 스마트카드와 같은 하드웨어 키 저장소에 개인키를 저장할 수 있으므로 클라이언트는 키 쌍을 기반으로 모든 공개 키 암호화 작업을 수행한다.

#### 4.2.3.1 CSP 설치절차

신화CSP를 설치하기 전에 먼저 카드리더기를 컴퓨터에 인식시키기 위해 장치 드라이버를 설치한다.

졸업 작품에 사용된 카드 리더기는‘GemPlus’사의 제품인‘GemPC410’이다.



<그림 38. 카드리더기 설치화면>

또한, 스마트카드에 사용 되는 CSP는 각 회사별로 틀리므로, 사용되어질 스마트카드 회사의 CSP를 사용해야 된다.

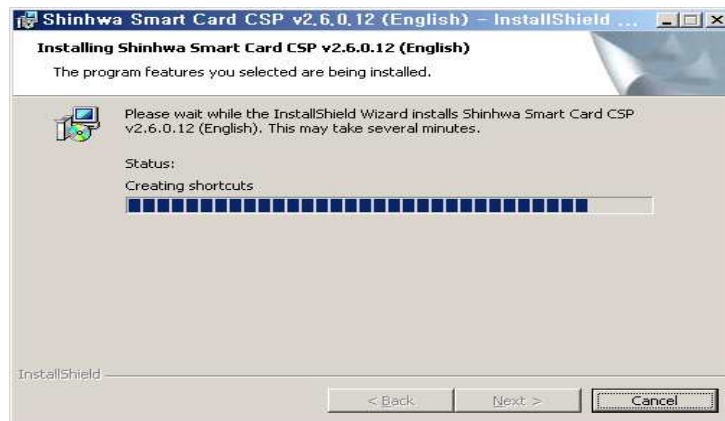
이번 AD구축 과정에서 사용될 CSP는 신화정보 시스템(주)의‘신화 SH-CSP’이다.

설치 CD 실행화면에서 ‘신화 카드리더기’ 인식프로그램과 ‘CSP’ 인스톨 버튼과 관리자 가이드가 보인다.



<그림 39. CSP설치 메뉴화면>

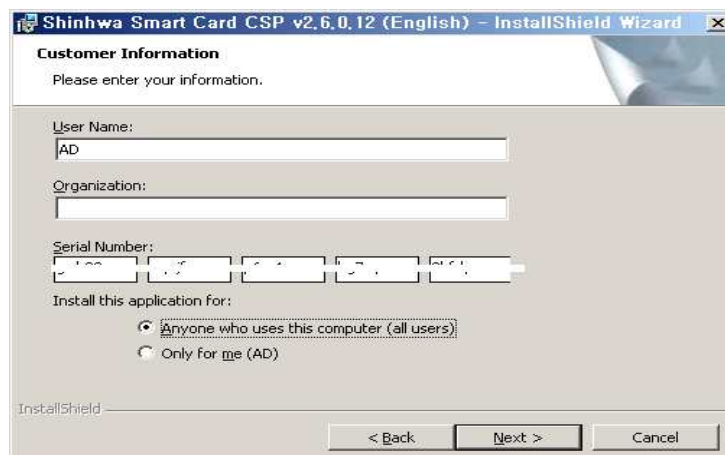
- 다음 CSP 인스톨 버튼을 누르면 설치가 시작된다.



<그림 40. 신화 CSP 설치화면>

#### 4.2.3.2 CSP 설치방법

- 설치안내에 따라 CSP를 설치하면 된다.

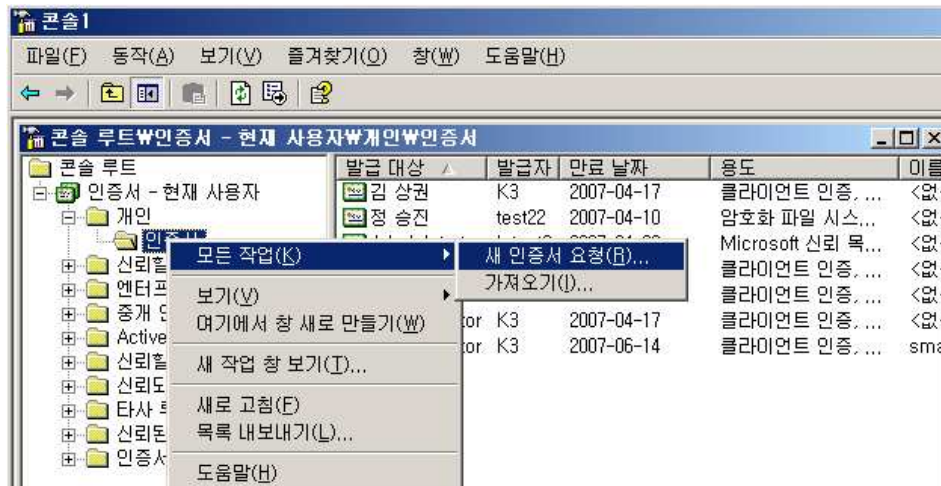


<그림 41. 신화 CSP 사용자명과 제품 키 입력>

## 4.2.4 인증서 신청 절차 및 방법

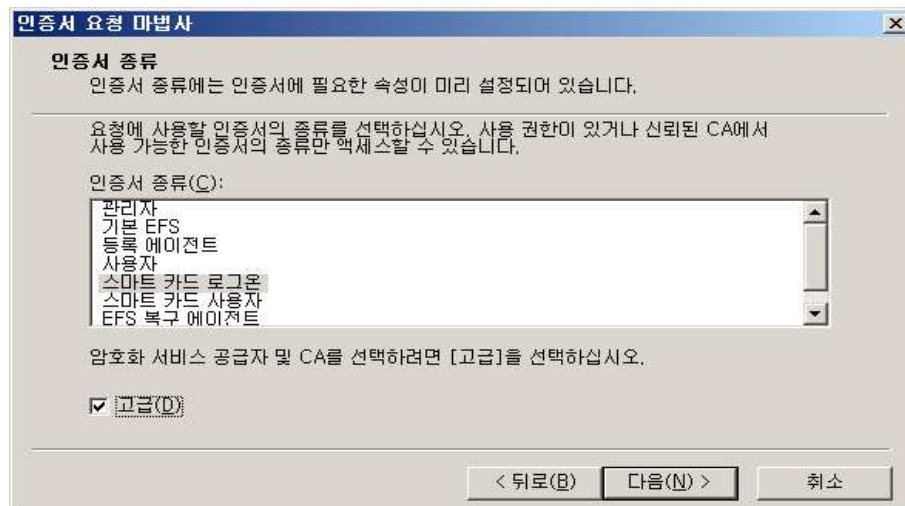
### 4.2.4.1 스마트카드 인증서 신청 절차

- 스마트카드를 사용하기 위해선 인증기관설치 과정에서부터 설정을 해두어야 한다. 관리자가 직접 발급해주는 경우에 다음과 같은 절차를 거친다.



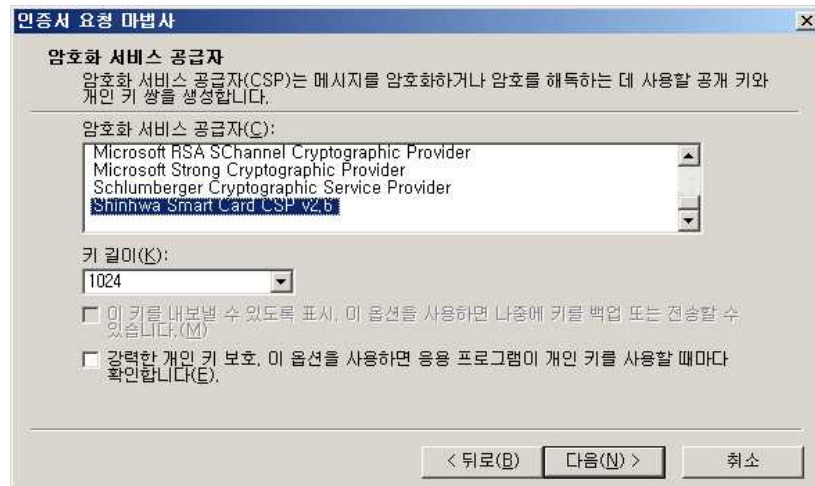
<그림 42. 스마트카드 인증서 요청>

- 인증서 종류로는 스마트카드 로그인 인증서를 선택한다.



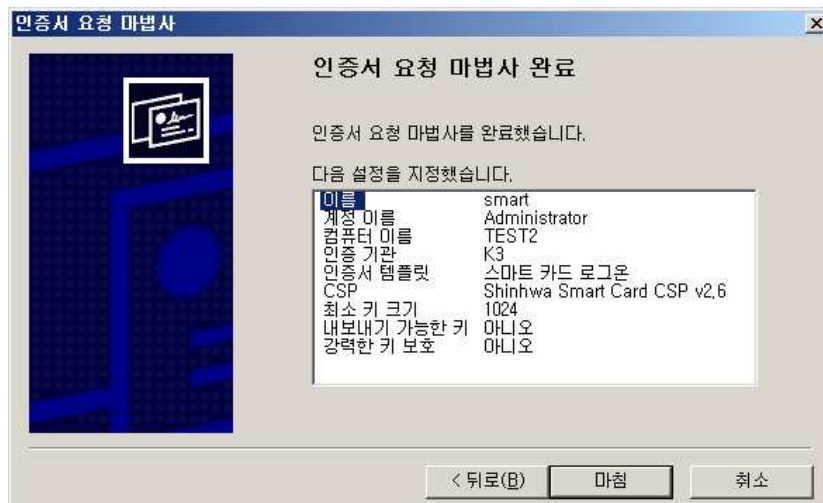
<그림 43. 스마트카드용 인증서 종류 선택>

- 암호화 서비스 공급자는 사용할 스마트카드제조회사와 호환되는 CSP를 선택해야 한다. 이번 졸업작품에 사용된 스마트카드는 신화CSP를 사용하게 되어있어 신화CSP를 선택한다.



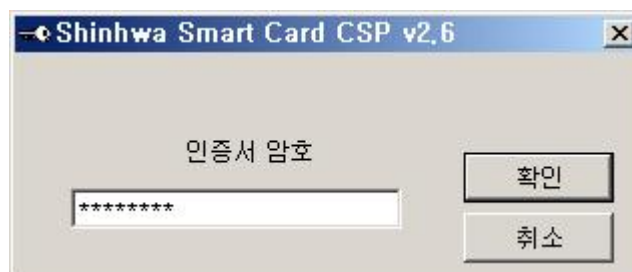
<그림 44. 암호화 서비스 공급자 선택>

- 인증서 요청 단계를 마치면 다음과 같이 입력정보를 확인하고 종료되어 진다.



<그림 45. 스마트카드 인증서 요청 완료>

- 인증서요청이 완료되면 사용되어질 카드를 리더기에 삽입하고 인증절차를 위해 카드의 PIN 번호를 입력하면 스마트카드 등록절차가 모두 끝나게 된다.



<그림 46. 스마트카드 PIN 입력>



- 스마트카드의 등록이 끝났으면 본래 목적인 Web에서의 사용을 위해 스마트카드 인증서를 웹에서 신청하고, 웹 로그인에 가능하도록 웹에서 '인증서 요청'을 선택한다.

#### Microsoft 인증서 서비스 -- SPs

##### 환영합니다.

이 웹 사이트를 사용하여 웹 브라우저, 전자 메일 클라이언트, 또는 다른 프로그램에서 사용할 인증서를 요청 사용자 자신을 안전하게 확인시키고, 전자 메일 메시지를 암호화 또는 서명할 수 있습니다. 또한 요청하는 인증서, 인증서 체인, 또는 CRL(인증서 해지 목록)을 다운로드

또한 이 웹 사이트를 사용하여 CA(인증 기관) 인증서, 인증서 체인, 또는 CRL(인증서 해지 목록)을 다운로드

인증서 서비스에 대한 자세한 내용은 다음을 참조하십시오. [인증 서비스 문서](#).

##### 작업 선택:

[인증서 요청](#)

[대기 중인 인증서 요청의 상태 표시](#)

[CA 인증서, 인증서 체인 또는 CRL 다운로드](#)

<그림 47. Web에서의 스마트카드 인증서 신청 화면 >

- 일반적인 AD 구조에서는 사용자인증서를 선택하여 인증서를 발급받으면 되나, 보안을 위해 스마트카드를 사용하는 경우에는 고급 인증서 요청을 선택해야 한다.

#### Microsoft 인증서 서비스 -- SPs

##### 인증서 요청

인증서의 형식 선택:

[사용자 인증서](#)

제출: [고급 인증서 요청](#).

<그림 48. Web에서의 스마트카드 인증서 요청 >

- 고급 인증서 요청 세부사항에서 '스마트카드 등록 스테이션...'을 선택한다.

#### Microsoft 인증서 서비스 -- SPs

##### 고급 인증서 요청

CA의 정책은 사용자가 요청할 수 있는 인증서의 형식을 결정합니다. 다음 옵션 중 하나를 선택하여 CA에 요청을 만들어 제출합니다.

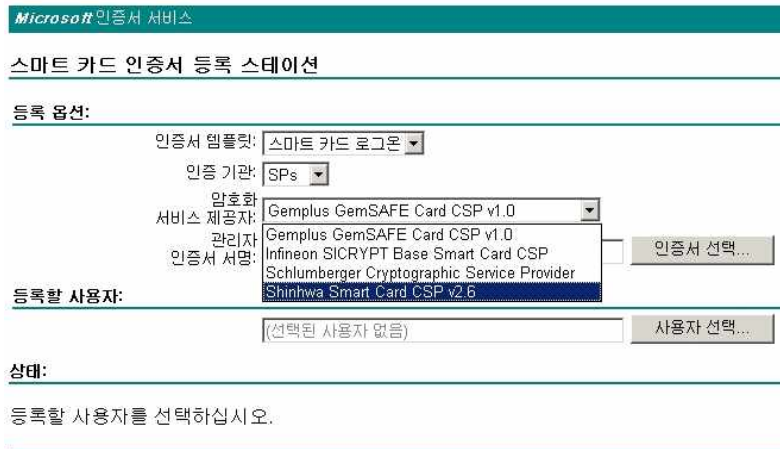
[Base 64 인코딩 CMC 또는 PKCS #10 파일을 사용하여 인증서 요청을 제출하거나 Base 64 스마트 카드 등록 스테이션을 사용하여, 다른 사용자 대신 스마트 카드를 위한 인증서를 요청](#)

참고: 다른 사용자를 위해 요청을 제출하려면 반드시 등록 에이전트가 있어야 합니다.

<그림 49. WEB에서의 스마트카드 인증서 요청 >



- 스마트카드에 맞는 CSP와 인증서 서명자 선택하면 인증서를 스마트카드에 설치하게 되고 PIN 번호 확인절차를 거치게 된다.



Microsoft 인증서 서비스

스마트 카드 인증서 등록 스테이션

등록 옵션:

인증서 템플릿: 스마트 카드 로그인

인증 기관: SPs

암호화 서비스 제공자: Gemplus GemSAFE Card CSP v1.0

관리자: Gemplus GemSAFE Card CSP v1.0

인증서 서명: Infineon SICRYPT Base Smart Card CSP

등록할 사용자: Schlumberger Cryptographic Service Provider

Shinlwa Smart Card CSP v2.6

인증서 선택...

사용자 선택...

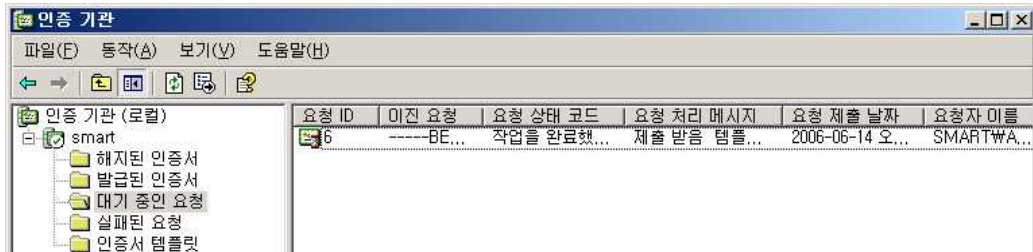
상태:

등록할 사용자를 선택하십시오.

<그림 50. Web에서의 스마트카드 인증서 등록 스테이션>

#### 4.2.4.2 인증서 발급 절차

- 스마트카드 인증서 발급 절차 : 관리자는 인증기관에서 대기 중인 인증서 요청을 요청자 확인 후 발급한다. Web에서 인증서 요청이 들어오면 이곳에서 인증서 발급 관리한다.



인증기관

파일(F) 동작(A) 보기(V) 도움말(H)

인증기관 (로컬)

smart

해지된 인증서

발급된 인증서

대기 중인 요청

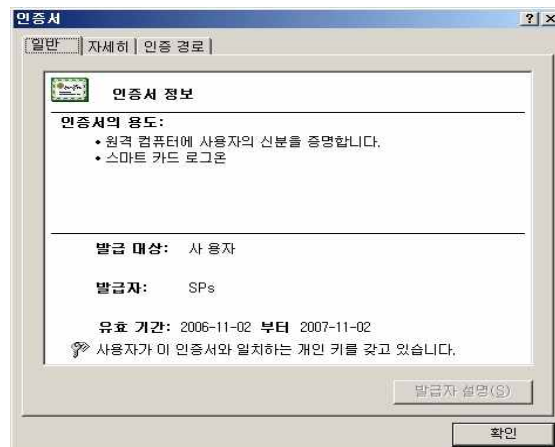
실패된 요청

인증서 템플릿

요청 ID	미진 요청	요청 상태 코드	요청 처리 메시지	요청 제출 날짜	요청자 이름
6	----	BE...	작업을 완료했...	제출 받음 템플...	2006-06-14 오... SMARTWA...

<그림 51. 스마트카드 인증서 발급>

- 스마트카드에 발급된 인증서 발급정보 확인



인증서

일반 자세히 인증 경로

인증서 정보

인증서의 용도:

- 원격 컴퓨터에 사용자의 신분을 증명합니다.
- 스마트 카드 로그인

발급 대상: 사용자

발급자: SPs

유효 기간: 2006-11-02 부터 2007-11-02

사용자가 이 인증서와 일치하는 개인 키를 갖고 있습니다.

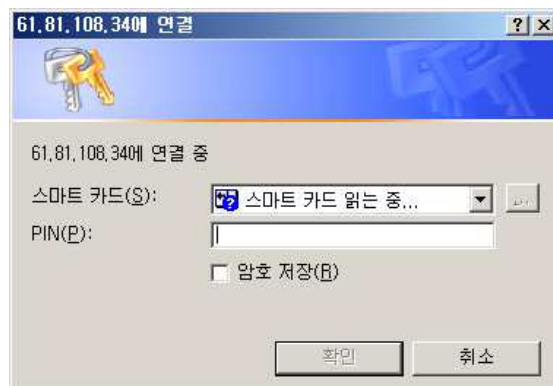
발급자 설정(S)

확인

<그림 52. 발급된 스마트카드용 인증서 정보>

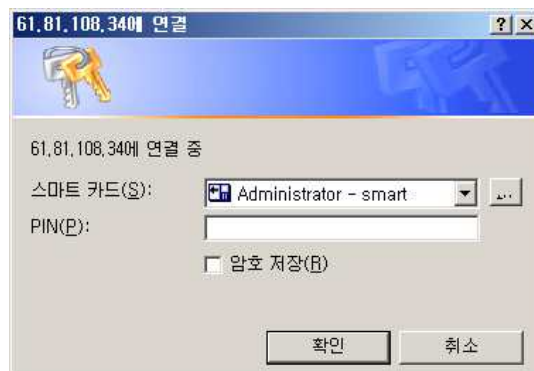
#### 4.2.4.3 인증서 사용 및 적용방법(WEB)

- 스마트카드 사용방법 : 강화된 보안성에도 불구하고 스마트카드 사용방법은 매우 단순하다. 스마트카드를 카드리더기에 삽입만 하면 된다.
- 스마트카드 삽입 후 화면



<그림 53. 스마트카드 인식>

- 스마트카드의 PIN을 입력하면 접속이 된다.

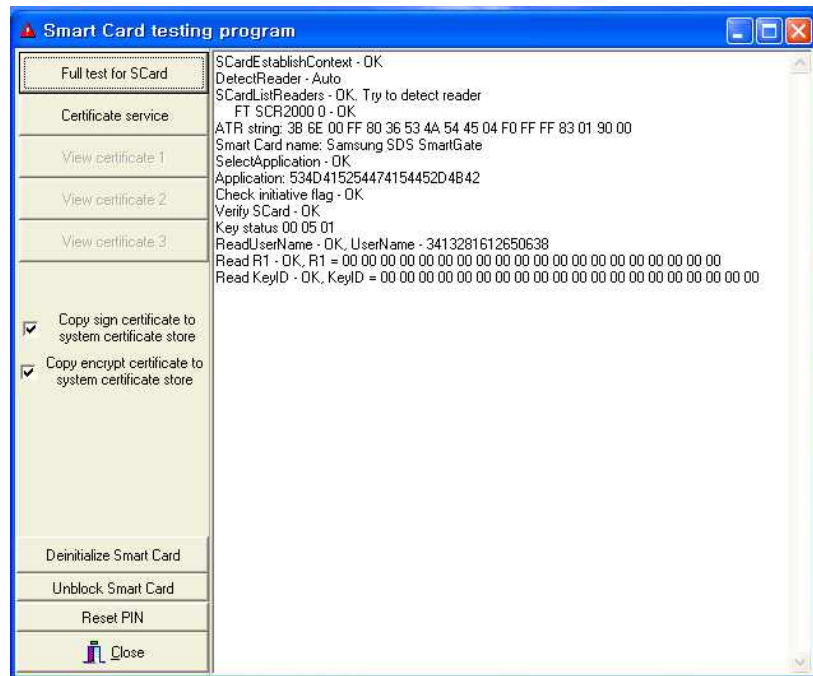


<그림 54. 스마트카드 로그인>

## 4.3 USB TOKEN의 구현

### 4.3.1 USB TOKEN

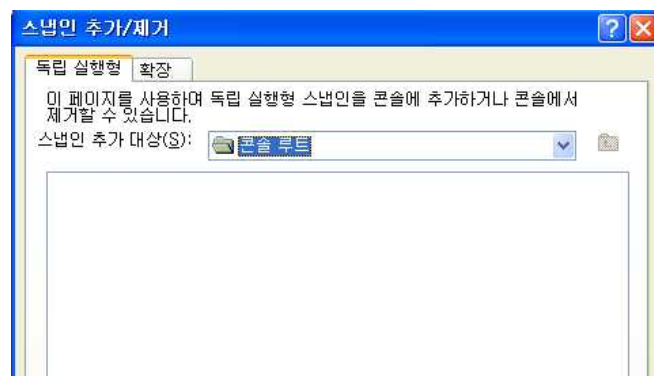
-USB TOKEN 드라이버 설치 후, 스마트카드 테스트 프로그램으로 USB 토큰 인식여부 및 정상작동 유무 확인.



<그림 55. USB 토큰 작동확인>

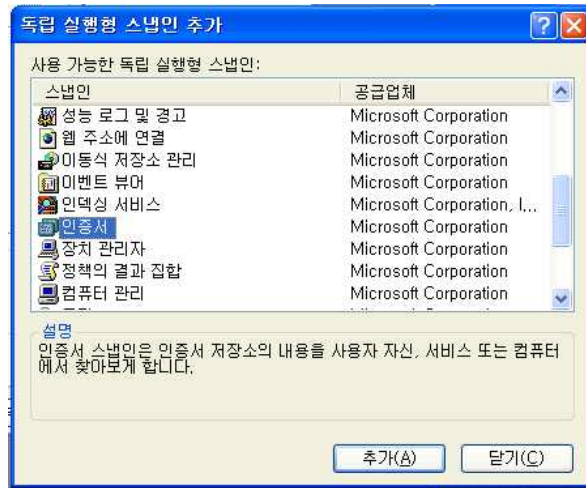
### 4.3.2 USB 토큰용 인증서 준비과정

- 실행 - MMS를 실행하여 스냅인 추가제거를 실행시킨다.



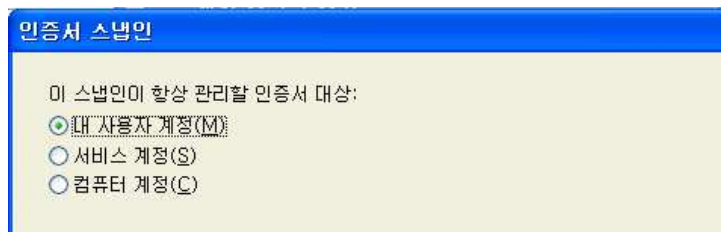
<그림 56. 신규 USB토큰 스냅인 추가>

- USB 토큰용 으로 사용되어질 스냅인 추가



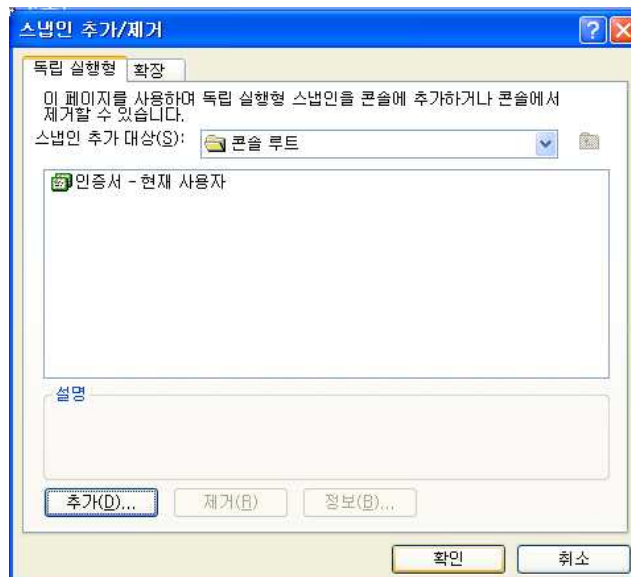
<그림 57. 인증서 추가>

- 스냅인이 관리할 인증서 대상 선택



<그림 58. 관리될 인증서 대상 선택>

- 생성한 인증서를 시스템에 추가하고 사용자를 선택하여 적용시킨다.



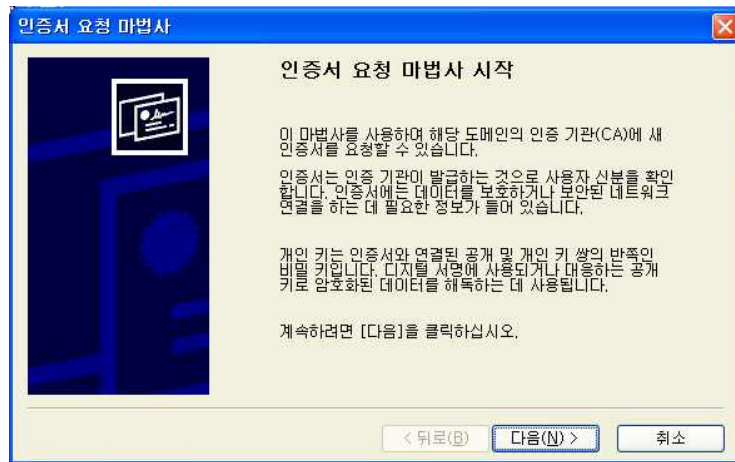
<그림 59. 인증서 생성>

- 시스템에서 관리되어질 개인사용자들의 인증서 신청 방법.



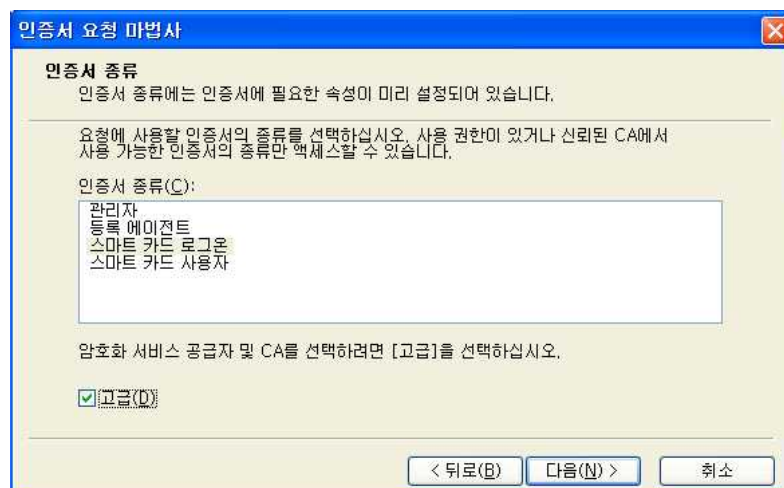
<그림 60. 개인 인증서 신청>

- 개인사용자용 인증서 요청을 위해 인증서 요청마법사를 실행한다.



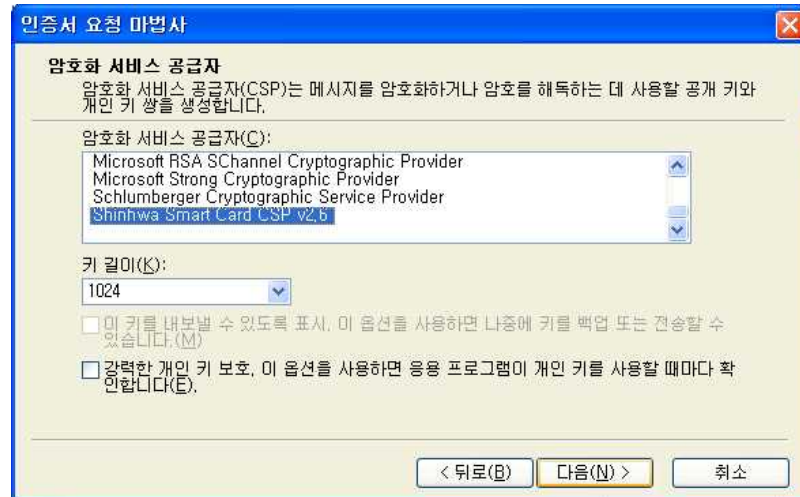
<그림 61. 인증서 요청 마법사>

- USB 토큰역시 내부에 스마트카드와 동일한 구조의 칩을 내부에 장착하고 있기 때문에 스마트카드와 동일한 유형으로 인증서를 요청한다.



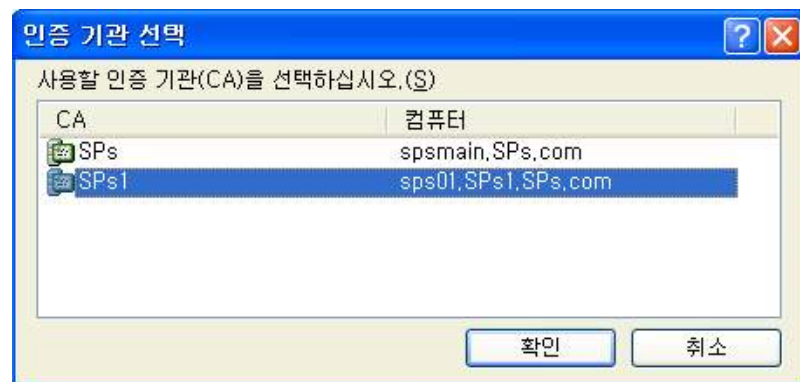
<그림 62. 스마트카드 로그인 선택>

- 암호화 서비스 공급자를 선택해야 하는데, USB토큰 역시 제품에 맞는 CSP를 선택한다.



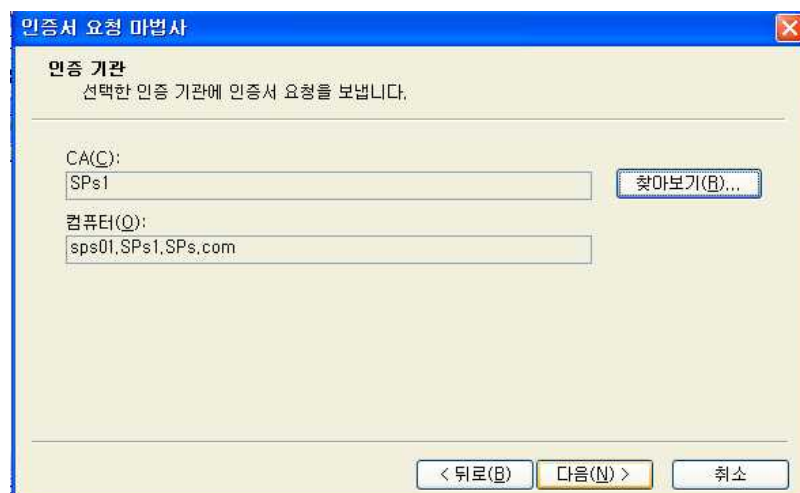
<그림 63. CSP 선택>

- CSP를 선택 하고난 뒤 사용할 인증기관을 선택한다.



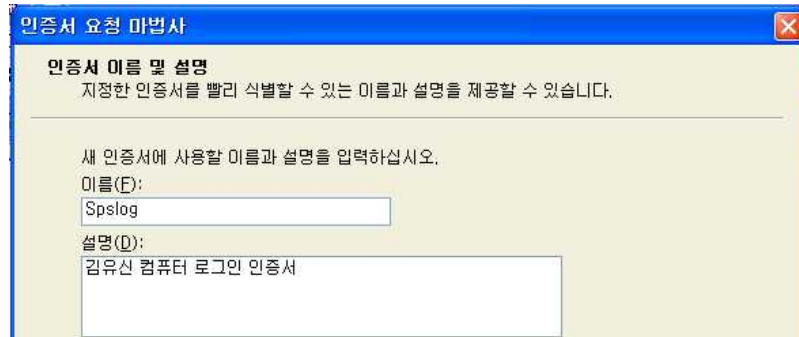
<그림 64. 사용할 인증기관 선택>

- 인증기관에 인증서 요청을 보낸다.



<그림 65. 인증서 요청>

- 인증서 요청시 인증서 이름과 인증서 설명을 기입 할 수 있다.



<그림 66. 인증서 이름 및 설명 입력>

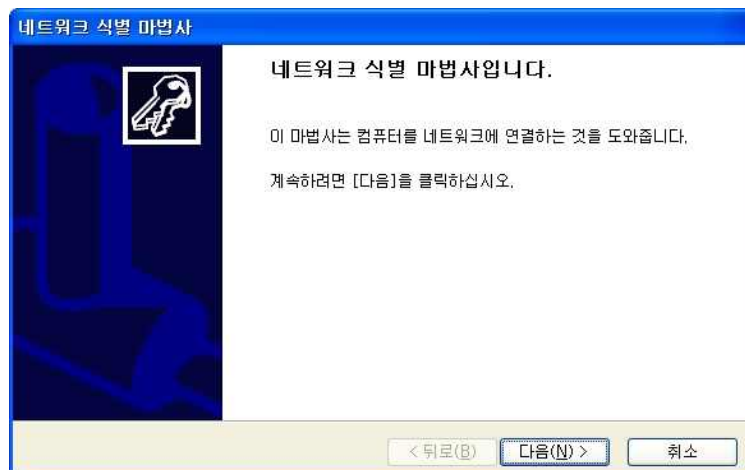
- 인증서 요청이 완료되면서 USB토큰의 PIN 번호를 입력하여 확인절차를 거친다.



<그림 67. USB토큰 PIN번호 확인>

#### 4.3.3 등록된 USB토큰 사용방법

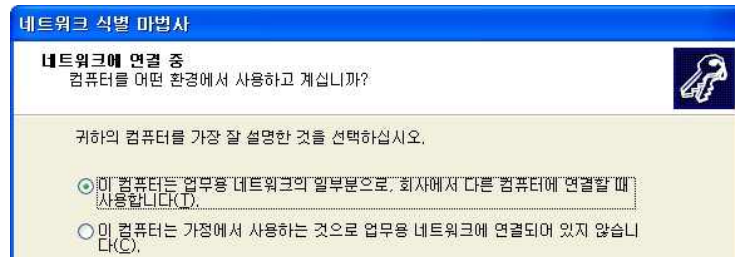
- 개인 사용자의 컴퓨터의 속성화면에서 네트워크 ID 탭을 선택하면 아래의 네트워크 식별 마법사가 실행된다.



<그림 68. 네트워크 식별 마법사>

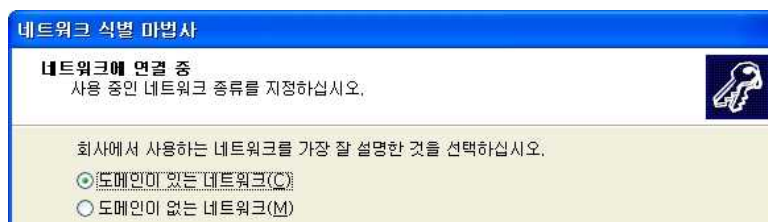


- 개인사용자인지 회사의 일원으로써 네트워크에 가입하는지를 선택하는 화면이다, SPs 도메인에 추가될 것이기 때문에 ‘업무용 네트워크...’를 선택한다.



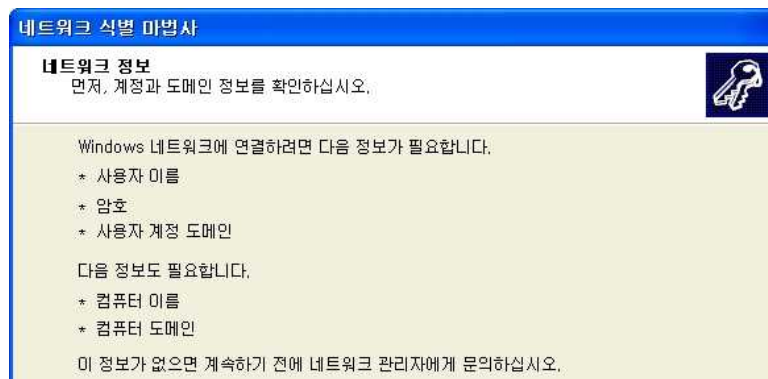
<그림 69. 네트워크 종류 선택>

- 도메인이 있는 네트워크의 사용자를 추가시키는 것이므로 도메인이 있는 네트워크 선택



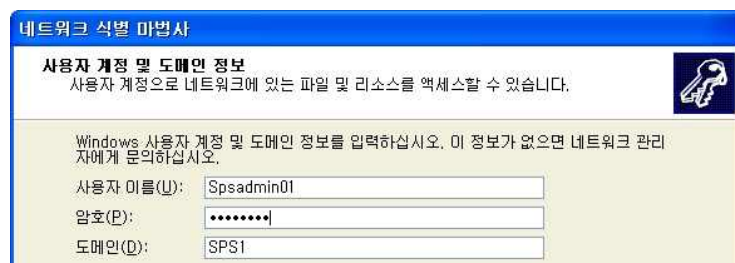
<그림 70. 도메인 선택>

- 네트워크에 계정이 미리 등록되어있는지를 확인하는 화면이다.



<그림 71. 사용자 계정 등록 확인>

- 사용할 계정명과 암호 도메인을 선택한다.



<그림 72. 사용자 계정 및 도메인 정보 확인>

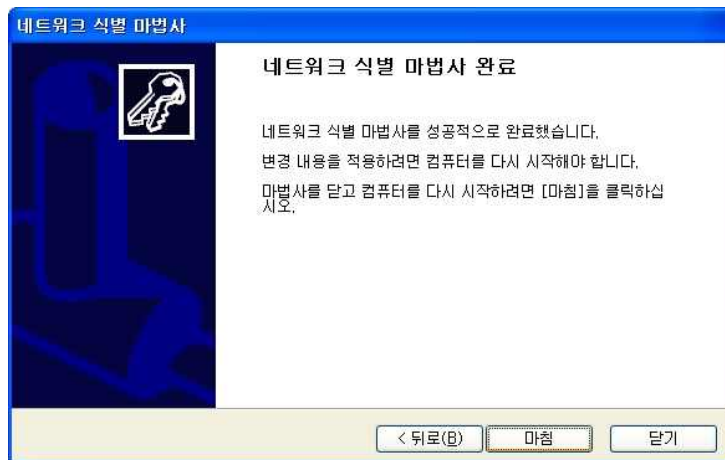


-컴퓨터를 사용할 사람의 권한을 설정하여 주는 화면이다.



<그림 73. 등록될 사용자 접근권한 선택>

-모든 설정이 끝나고 채부팅을 하면 네트워크에 주어진 ID와 패스워드를 입력하거나 USB 토큰을 삽입하고 로그인 하면 된다.



<그림 74. 네트워크 식별 완료>

#### 4.3.4 Web에서 인증서 발급 절차

- 인증서 발급 Web페이지에 인증서발급관리자 계정으로 로그인 한다.



<그림 75. Web 접속>

- 스마트카드 인증서 요청방식과 동일하게 인증서 발급 요청한다.

**Microsoft 인증서 서비스 -- SPs1**

---

**고급 인증서 요청**

---

**인증서 템플릿:**

관리자 ▼

---

**키 옵션:**

☒ 새 키 집합 만들기    ☐ 현재 키 집합 사용

CSP: Microsoft Enhanced Cryptographic Provider v1.0 ▼

키 사용: ☒ 교환

키 크기: 1024    최소: 384    최대: 16384    (공통 키 크기: 512 1024 2048 4096 8192 16384)

☒ 자동 키 컨테이너 이름    ☐ 사용자 지정 키 컨테이너 이름

☒ 키를 내보낼 수 있게 표시  
☐ 키를 파일로 내보내기  
☐ 강력한 개인 키 보호 사용  
☐ 인증서를 로컬 컴퓨터의 인증서 저장소에 저장  
     *인증서를 사용자의 인증서 저장소 대신에 로컬 컴퓨터의 저장소에 저장합니다. 루트 CA의 인증서를 저장하지 않습니다. 로컬 컴퓨터 저장소의 키를 생성 또는 사용하려면 관리자의 권한이 있어야 합니다.*

---

**추가 옵션:**

요청 형식: ☒ CMC    ☐ PKCS10

해시 알고리즘: SHA-1 ▼  
     *서명 요청에만 사용됩니다.*

☐ 요청을 파일에 저장

<그림 76. USB토큰 인증서 요청>

- 인증서 등록 준비

**Microsoft 인증서 서비스**

---

**스마트 카드 인증서 등록 스테이션**

---

**등록 옵션:**

인증서 템플릿: 스마트 카드 로그인 ▼

인증 기관: SPs1 ▼

암호화 서비스 제공자: Shinhwa Smart Card CSP v2.6 ▼

관리자 인증서 서명: Administrator    인증서 선택...

---

**등록할 사용자:**

(선택된 사용자 없음)    사용자 선택...

<그림 77. 인증서 등록>

- USB토큰을 사용할 사용자 선택



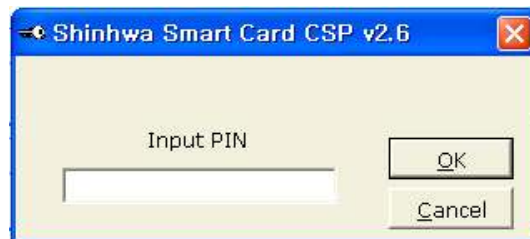
<그림 78. 사용자 선택>

- 사용자 선택 후 다음버튼을 누르고, USB토큰의 PIN 번호를 입력한다.



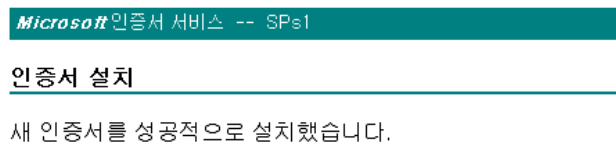
<그림 79. 인증서 요청정보 입력 완료>

- USB토큰 PIN 번호입력.



<그림 80. PIN 번호 입력>

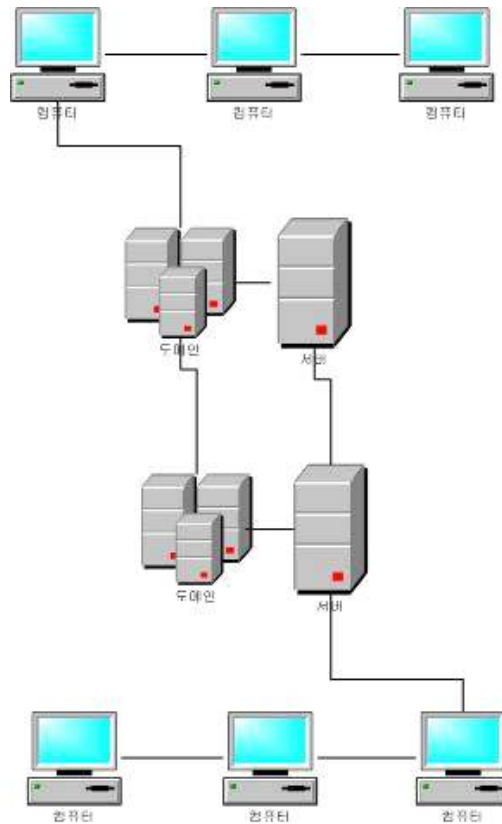
- 인증서가 발급되어 USB토큰에 설치되면 다음의 화면이 출력되고 USB토큰으로 Web로그인이 가능하다.



<그림 81. 인증서 발급 및 설치 완료>

## 5. 결과 및 분석

### 5.1 통합 인증 관리 시스템의 동작 과정



<그림 82. 통합 인증 관리 시스템의 구성>

본사의 메인 서버에서 하위 인증 서버로의 권한 부여로 인해 메인 서버 및 하위 인증 서버가 클라이언트(사용자)에 대한 인증 요청 및 부여, 관리에 대한 처리 및 관리를 보다 용이하게 설계할 수 있다. 지사 서버에 속한 클라이언트(사용자)들은 최초 지사 서버에 인증을 요청한다. 지사 서버는 지사 클라이언트의 인증 요청에 대해 심사 후 승인을 한다.

지사 서버는 최초 본사 서버에게 인증 권한을 부여 받아 하위 인증 서버의 권한을 얻는다. 하지만 지사 서버는 다른 하위 인증 기관을 인증해 줄 권한은 없다.

각 서버에 대한 클라이언트들은 소속 서버에 인증 요청 후 승인을 얻어 개인이 소유하고 있는 스마트카드 및 USB 토큰의 IC칩에 인증서를 인식시켜 로그인시 사용한다. 클라이언트들은 기존의 아이디와 문자 조합의 패스워드로 로그인 하는 것이 아닌 IC칩을 사용하는 스마트카드를 이용하여 보다 높은 보안 서비스를 제공 받는 것이다.

## 6. 결론

앞서 구현해 보았던 스마트카드 인증 로그인 방식은 크게 두 가지의 기능을 제공하였다. 하나는 인증서가 설치된 서버 관리자의 신원확인 기능이며, 다른 하나는 클라이언트(사용자)와 서버간의 안전한 보안 인증이 가능하였다.

개인의 신원확인이라는 것으로써 인증서를 발급하고 그것을 소유하고 있는 서버에 대한 엄격한 심사를 거치기 때문에 더 나은 보안이 가능하였다. 이는 인증기관의 신뢰성과 사용자의 보안이 좀 더 강화 되었다고 볼 수 있었다.

회사의 서버와 직원간의 사용자 인증을 가능하게 하는 기능은 스마트카드 내부의 인증서와 서버에 인증되어 있는 개인키 확인 기능을 이용하는 것으로 서버 인증센터가 설치되어야 한다. 그래서 사용자의 민감한 정보 등을 다루는 개인 컴퓨터에 사용자의 데이터 보호를 위해 타인의 로그인 방지를 위하는 것으로 스마트카드 및 USB토큰 로그인 방식을 구현해 봄으로써 더 나은 인증 서비스를 제공할 수 있었다.

개인 정보 보안에 힘쓰고 외부 인원의 정보 도용을 막는데 힘쓰는 이 시기에 실질적으로도 IC칩이 탑재된 스마트카드와 USB토큰을 이용한 인증 방식은 안정된 서비스를 위해 많은 개발에 힘쓰며 이에 따라 널리 쓰이는 추세에 있다. 얼마전 우리나라의 대기업 삼성에서도 VISA와 손잡고 스마트카드의 개발에 들어갔으며 이는 앞으로의 IC칩 내의 정보의 안전성을 간접적으로나마 얼마나 중요한지 알 수 있다.

하지만, 스마트카드라 해도 내부 정보를 전부 지킬 수 있는 구조로 되어 있는 것은 아니다. 분실로 인한 내부의 정보를 부정하게 읽어내는 수법도 있다는 것이다. 이러한 것에 대비해 내부 정보를 고도로 암호화하는 등의 대책을 세워, 용도에 따라 필요한 보안 대책들을 수립한다면 보다 완벽한 인증 메커니즘으로 자리 잡을 수 있을 것이다.

## 7. 참고문헌

1. (Mastering)Windows Server 2003 / Mark Minasi 외 공저
2. Active directory using bible
3. MCSE : Windows 2000 network infrastructure administration study guide  
/ Paul Robichaux ; James Chellis
4. Configuration Microsoft Certificate Authority and domain controllers for use of  
system SHINHWA WINDOWS-LOGON SYSTEM PACK 1.0  
/ MS word document
5. Microsoft Official Course 2078A / Microsoft
6. 정보보호 프로젝트 실무 (Windows 보안가이드)