공개키 기반 구조에서 KT Single Sign-On 설계
(Design of KT's Single Sign-On on Public Key Infrastructure)

연 승 호 † 박 현 규 † 오 희 수 † 김 영 헌 † 전 병 민 ††
(Seung-ho Yeon) (Hyun-Gyu Park) (Hee-Soo Oh) (Yeong-Heon Kim) (Byoung-Min Jun)

요 약 본 논문은 인증서를 기반으로 한 SSO(Single Sign-On)를 구현함에 있어 LDAP(Lightweight Directory Access Protocol)의 DN(Distinguished Name)과 속성(Attribute)을 지정함에 따라 다양한 응용서비스들을 수용할 수 있는 데이타 구조를 설계하였다. 조직의 인사데이타를 바탕으로 LDAP 데이타를 구축하고, 수시 변경되는 자료에 대하여는 연동에 의한 지속적인 자동수정 기능을 적용하였다. 또한 인증서 발급을 위해서 PKI(Public Key Infrastructure) 기반의 CA(Certificate Authority) 서버를 적용하였으며, 인증통신을 위한 데이타 암호화는 SSL(Secure Socket Layer) 기반의 SHTTP(Secure Hyper Text Transfer Protocol)을 적용하였다.
키워드 : 공개키, 인증서

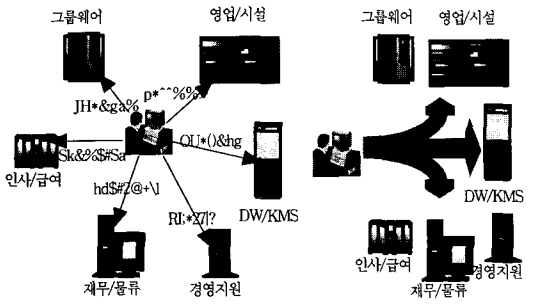
Abstract This paper gives a comprehensive overview of the SSO solution design on the intranet. SSO described in this paper is based on LDAP, PKI and CA. We designed the data structure to hold many various application services by changing the attribute and DN of LDAP DB. We built LDAP DB using the employee records stored in our organization database. LDAP DB is routinely updated from the database. CA Server that depends on PKI is used to issue the certificates. SHTTP based on SSL is used to protect the data between certificate server and the intranet users.
Key words : PKI, SSO, LDAP

1. 서 론

사용자 인증에 의한 서비스를 제공하는 인터넷/인트라넷 웹 사이트에 접속하면 사용자ID와 패스워드를 요청받는 경험을 했을 것이다. 인터넷 사용의 급증에 따라 대부분의 사용자들은 여러 웹 서버의 서비스를 사용하고 있고 서로 다른 웹 서버에 접속할 때마다 서로 다른 사용자ID와 패스워드를 입력해야 한다. 특히 인트라넷에서는 회사내의 서비스별로 사용자ID를 관리하고 있어 한 서버에 접속하여 회사에 속한 사원임을 인증받았다 해도 다른 서버에 접속하면 같은 방식의 인증 확인 절차를 반복하거나 심지어 서버마다 ID와 패스워드가 달라 사용자의 혼선을 초래하기도 한다. 이러한 문제점을 해결하기 위하여 SSO 기술이 사용되는데, SSO란 한번의 로그인을 통해 모든 서버에 접속할 수 있는 권한을 갖게하는 개념이다. SSO 구현을 위한 방법으로는 기존 ID/Password 방식이 구현하기가 용이하나 사용자의 인증정보들이 네트워크상에서 노출될 가능성이 많기 때문에 X.509에 의한 인증서(Certificate) 기반의 강력한 인증(Strong Authentication) 기법이 적용되고 있다[1-3]. 또한 SSO를 적용한 솔루션의 형태는 SSO 본연의 기능인 통합 로그인 기능에서 인증정보 유지, 개인화 서비스 제공, 다양한 관리기능 등이 포함되며, 접근권한관리 기반구조인 PMI(Privilege Management Infrastructure)와 함께 통합되어 EAM(Extranet Access management)으로 확대 발전되고 있다.

기존의 SSO 관련 기술들을 분석하면 가장 쉬운 방법으로 SPUR(Single Point of User Registration) 방식은 강제적으로 한군데에서 사용자 등록관리를 하게 한 방법으로 다양한 응용서비스를 수용함과 보안의 신뢰를 보장하기가 어렵다. 또한 패스워드 동기화 방식은 응용

† 비 회 원 : 한국통신 멀티미디어연구소 연구원
shyeon@kt.co.kr
autosys@kt.co.kr
ohhs@kt.co.kr
yhkim@kt.co.kr
†† 종신회원 : 충북대학교 컴퓨터공학과 교수
bmjun@cbucc.chungbuk.ac.kr
논문접수 : 2000년 3월 29일
심사완료 : 2001년 11월 21일



(a) 기존 시스템 환경 (b) SSO 적용 환경

그림 1 기존의 정보시스템과 SSO 적용시스템

프로그램간 패스워드를 통일 시키는 방식으로 패스워드 동기화에 따른 통일성 유지의 위험 부담과 보안의 신뢰성 보장이 어렵다. 좀더 강력한 방법으로 Kerberos 방식이 있으며 최근에는 지문, 홍채 등을 이용한 여러 가지 생체인식 방식들이 연구 및 개발되고 있다.

본 논문에서의 공개키 기반 인증서 방식은 기반 시스템 구축에 초기 투입비용이 발생할 수 있으나 보안성이 강조되고 있는 현실에서 다양한 응용프로그램들을 수용하기 위한 방안으로 주목받고 있다. 특히 디렉토리 시스템인 LDAP 서버를 중심으로 인증서를 CA에서 받는 방식으로 응용프로그램과 SSO 서버 사이의 API 메커니즘을 이용한 여러 가지 구현 시스템들이 나오고 있다. 특히 X/Open의 XSSO를 필두로 하여 표준화 되지는 않았지만 SESAME(A Secure European System for Applications in a Multi-vender Environment), Netscape Suitspot, Novell 등에서 SSO 모델을 제시하고 있다[4-5].

논문은 총 5장으로 구성되며, 2장에서는 SSO를 구현함에 있어서의 구성요소를 분석하고, 3장에서는 SSO를 구현하기 위한 모델을 설정하였다. 4장에서는 LDAP과 인사DB등을 이용한 시스템 구현을 기술한 후 5장에서 결론으로 끝을 맺는다.

2. SSO 구성요소

강력한 인증기법을 이용한 SSO 시스템에는 인증서에 의한 사용자 인증 메커니즘, LDAP에 의한 접근제어 및 내부사용자 정보관리, 클라이언트와 서버간의 데이타 암호화를 위한 통신보안 기술 등이 필요하다.

2.1 사용자 인증 메커니즘

공개키 기법에 의한 상대 인증은 각 이용자가 비밀로 보유하고 있는 비밀키와 그것에 대한 검증용 공개키가 있어서 이용자는 자기의 비밀 정보를 밝히는 것이 아니고, 검증자와 통신교환에 의해 공개키에 대응하는 비밀키를 갖고 있는 것을 증명하는 기법이다. 공개키 기법에 의한 상대 인증은 공개키 암호방식, 영지식 증명을 이용한 방식, 3교신 프로토콜, ID에 근거한 인증방식 등이 있으며 공개키 암호화 원리는 다음과 같다[6-11].

[1] 키생성 및 등록 : 이용자 A는 자신이 비밀로 관리하는 비밀키 S_A와 공개키 P_A의 쌍을 정해진 방법으로 생성한다. A는 P_A를 공개키 디렉토리에 등록한다.

[2] 암호화 : 다른 이용자 B가 A에게 암호화 하는 경우를 생각한다. B는 공개키 디렉토리를 사용해 A의 공개키 P_A를 검색한다. 다음으로 메시지 m을 P_A를 사용하여 암호화 한다. 여기에서 암호문 c를 $E_{P_A}(m)$으로 표시한다.

$$c(\text{암호문}) = E_{P_A}(m) \quad (1)$$

[3] 복호화 : 암호문 c를 받은 A는 자신만이 알고 있는 비밀키 S_A를 이용해 c로부터 $m = D_{S_A}(c)$를 복호한다. $m = D_{S_A}(E_{P_A}(\mathrm{m}))$이 성립하는 것에 의해 복호가 행하여진다.

$$m(\text{평문}) = D_{S_A}(c) = D_{S_A}(E_{PA}(\mathrm{m})) \quad (2)$$

또한 공개키를 이용한 상대 인증 방식은 그림 2의 절차와 같다.

[1] 공개키를 사용하는 모든 사용자는 공인된 기관에 자신의 공개키 P_A를 등록해 둔다.

[2] 송신자는 난수 r을 생성해서 수신자의 공개키 P_A를 이용하여 r을 암호화 한다. 그리고 암호문 $c = E_{P_A}(r)$을 이용자에게 보낸다.

[3] 수신자는 자신만이 아는 비밀키 S_A를 이용하여 $t = D_{S_A}(c)$를 구하므로써 송신자를 인증하고, 다시 t를 자신의 키로 암호화하여 송신자에게 보낸다.

[4] 송신자는 $t = r$ 인지 검증하고 성립하면 정당한 사용자로 인증한다.

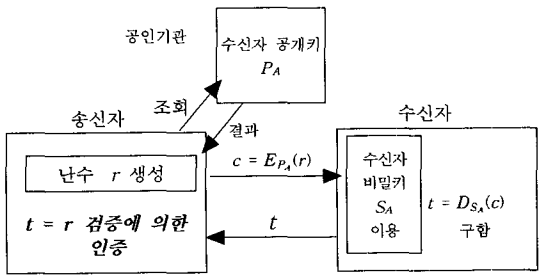


그림 2 공개키에 의한 상대인증

2.2 LDAP 사용자 정보관리

인증정보에 대한 데이타를 관리하기 위해서는 DBMS와 LDAP을 이용하여 관리할 수 있다. LDAP은 DBMS에 비하여 트리 형태의 데이타 구조를 사용하기 때문에 계층적 구조를 자동유지하며, Object가 데이타 구성의 기본 개념으로 사용되고, 탐색 능력이 우수하고 응답속도가 빠르기 때문에 본 논문에서는 인증정보를 관리하는 도구로 선택하였다. 또한 LDAP은 사용자 및 자원에 대한 접근제어를 다양하게 부여하여 적절한 접근 권한을 가진 Enterprise Repository를 구현할 수 있다. 그리고 Replication 로직을 자동 제공하고, 트리 구조인 데이타를 수많은 작은 가지로 나누어 서버를 분산할 수 있으며 분산 DB 모델을 구현할 수 있다[12-13].

3. SSO 메커니즘

일반적으로 인증서에 기반한 SSO에 대한 동작 관계를 서버 쿠키와 세션 관리를 적용하면 그림 3과 같은 SSO 메커니즘으로 나타낼 수 있다. 사용자가 인증서를 요청하여 발급 받아 보관 후 인증요구 및 토큰에 의한 접속 서비스 일괄을 수행한다. 3장은 SSO 동작 관계를 모듈을 통해서 살펴보고 각 모듈의 구성을 설명한다.

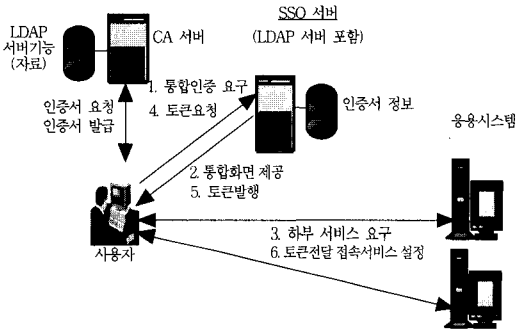


그림 3 SSO 동작 메커니즘

3.1 SSO 동작

SSO 서버(LDAP 서버 포함)를 중심으로 인증서 발급 및 철회 서버, 각종 응용프로그램 웹서버들을 사용자가 SSO로 처리하는 메커니즘을 그림 4와 같이 나타낸 것이다. 제안된 SSO 모델의 전체적인 흐름은 인증서 발급, LDAP 저장부분은 기존의 방식과 유사하다. 포탈 서비스 화면에서 같은 도메인 내의 서버들에 분산된 서비스로 이동을 위해 다른 서비스 메뉴를 선택하면 인증 통합메뉴에서 재인증 절차를 거치지 않고 SSO 서버에서 승인과정을 거치도록 하였다. LDAP Attribute에는 각 서비스마다 사용자 접근제어에 대한 정보를 갖고 있어서 서비스가 선택되면 접근권한이 부여된다. 또한 사용자마다 SSO 서버에 개인의 프로파일이 있어서 홈페이지를 구성하듯이 다른 서비스를 선택할 수 있는 통합메뉴를 갖고 있으며, 다른 서비스로 이동할 시에는 통합메뉴에서 선택하고 별도의 인증절차를 거치지 않는다. SSO 기본 구성요소간 연관관계 메커니즘은 다음과 같다.

(1)-(4)는 인증서 발급으로 일회성이다. Cookie와 같이 Session을 사용하면 사용자 정보를 일정시간 동일 도메인 내에서 전달할 수 있는 기능을 이용한 것으로 Session은 Property(SessionID, Timeout), Method (Abandon), Event(Onstart, Onend) 등의 일을 한다. 어떤 페이지라도 값을 제어할 수 있고, 다른 페이지로 이동하여도 값이 유지된다. 또한 일정 시간동안 사용하지 않으면 자동소멸하는 기능도 있다. 프로그램, 페이지 내에서 Action 처리를 위한 Routine을 포함하고 있어야 하며, Global로 선언하여 사용할 수 있다. 즉 Cookie는 인증서 정보를 유지하기 위한 수단으로 사용된다.

[인증서 발급]

(1) 사용자가 CA 서버에 접속하여 신청자 모드에서 인증서(전자신분증) 발급을 신청한다.

(2) 조직내의 구성원에 대하여 발급하고자 할 경우는 발급 신청시 입력한 사번(유일한 구분정보 : 학번, 주민등록번호)을 인사관리서버에서 검색하여 등록된 사용자에 한하여 발급 신청을 받는다.

(3) CA 서버 관리자가 CA 서버에 관리자 모드로 접속하여 인증서 신청 목록에서 (1)의 신청건을 접수하고 인증서를 발급한다.

(4) (1)의 신청자는 (2)의 발급과 동시에 신청시에 입력한 E-mail 주소로 인증서 발급 완료 메일을 받고 메일 안의 link 대로 수행하여 인증서를 자신의 PC에 다운로드 한다. 또한 CA 서버에서 자신이 신청한 인증서를 직접 다운로드해 갈 수도 있다.

[접속시도 및 연결]

(5) 사용자가 SSL-Enabled된 SSO 서버에 웹서비스를 받기 위하여 접속을 시도한다.

(6) SSO 서버에서 사용자 인증서 전송을 요구하고 웹 클라이언트가 PC에 다운로드되어 있는 자신의 인증서를 서버에 전송한다.

(7) SSO 서버가 사용자 인증서의 유효성을 체크한다.

(8) (6)이 통과되면 웹서버와 웹브라우저간의 데이타를 암호화 하는 SSL 연결이 설정된다.

[사용자 인증]

(9) 인증서 로그온 프로그램이 클라이언트로부터 전송

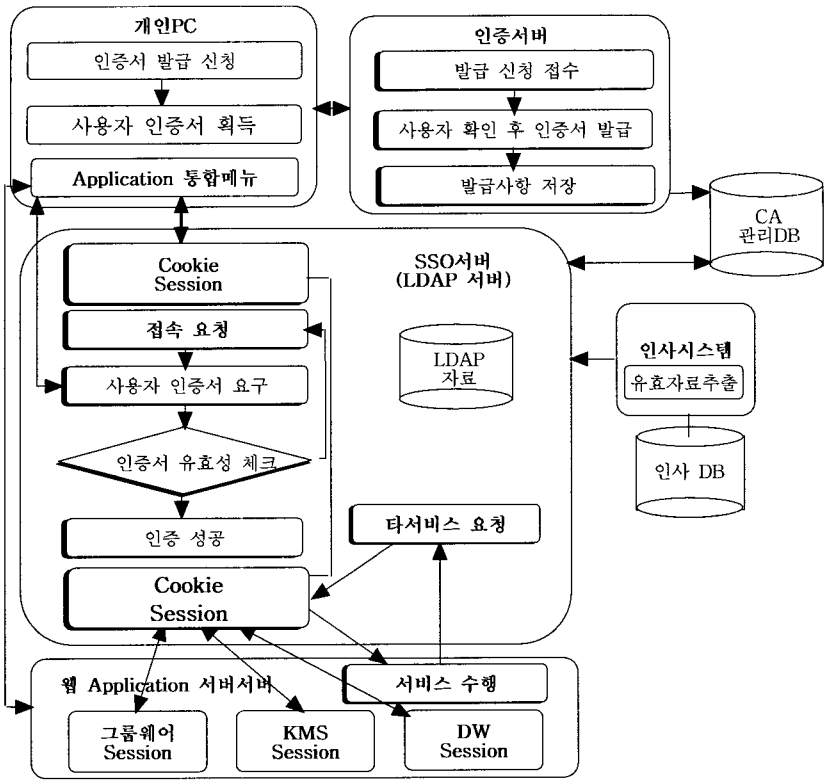


그림 4 SSO 모델 연관 관계

되어 온 인증서에서 사번을 추출하여 SSO 서버에서 등록된 사용자 여부를 검색한다.

(10) (9)가 통과되면 검색결과로 받은 로그온 사용자 암호와 사번(사용자 ID)을 응용프로그램 서버에 전송하여 사용자 인증을 통과한다. 이 과정이 끝나면 정상적인 서비스를 받을 수 있는 환경이 되고 사용자 초기 통합화면이 나타난다.

[접근권한 확인]

(11) 이때 SSO 서버 내에 저장되어 있던 ACL의 정보에 따라 해당 서비스의 접근권한을 체크하고 레벨에 따라 통제 받는다.

(12) 다른 응용프로그램 서비스를 받기 위해서는 사용자 클라이언트의 통합메뉴에서 해당 서비스를 선택한다.

[SSO 서비스]

(13) 이미 로그온한 정보는 쿠키로 갖고 있어서 다른 애플리케이션 서버에 접속할 때 활용한다. 다른 애플리케이션 서버에는 인증 완료된 쿠키 정보를 전달한다.

(14) Session 정보는 사용자마다 생성 및 소멸, 유지할 수 있으며 다른 웹페이지로 이동해도 없어지지 않고 사용자 정보를 가질 수 있기 때문에 정해진 시간내에 통합메뉴내에서 동일 도메인 내에 다른 서버의 프로그램을 기동할 수 있다.

(15) 다른 애플리케이션 서버의 서비스도 (12)에서와 같이 ACL 정보에 따라 접근 권한을 부여 받는다.

3.2 SSO 모듈 구성

클라이언트에는 윈도우즈 환경하에 SSL을 지원하는 웹브라우저가 준비된다. 사용자는 웹브라우저를 사용하여 여러 가지 서비스에 접속한다. 인증서(비밀키)는 CA 서버로부터 받아 놓는다. 사용자는 여러 가지 서비스 제공을 받기 위하여 SSO 서버에 개인 메뉴를 만들 수 있고 관리자가 통합메뉴를 제공할 수 있다. SSO 서버에는 웹서버 이외에 SSL 모듈의 소프트웨어를 별도로 설치하고 데몬 프로그램도 SSL을 지원하는 모드로 실행된다. 디렉토리 정보에는 사용자 정보와 조직정보, 사용자 각각에 대한 접근제어 정보와 인증서 정보를 갖는다. 사용자 관리는 LDAP 정보의 하나이지만 사용자 인증이 확정되면 클라이언트에 개별적인 화면을 제공한다. 메뉴는 응용프로그램 서버마다 다른 인증관계를 갖고 있기

때문에 Script로 조정할 수 있는 기능을 제공하며, Config는 개인 메뉴를 사용할 것인지 관리자가 제공한 메뉴를 사용할 것인지 설정하는 모듈이다. 관리자 관리는 웹서버, 사용자 정보 등의 DN과 Attribute를 관리하는 기능을 갖는다. 메뉴와 Config는 사용자가 관리하는 것과 유사 하지만 전체적으로 사용하는 기능이 사용자가 사용하는 기능보다 다양하다. Session을 이용한 보안은 사용자 정보를 일정 시간동안 저장할 수 있어서 다른 웹 페이지로 이동할 경우에 페이지 인증처리를 받을 수 있다. 응용프로그램 서버는 웹서버가 다를 수 있고 사용자 인증 모듈이 다를 수가 있다. 인증서에 의한 인증기능을 LDAP에 완전 의존하는 형태와 인증서 없이 사용자ID와 패스워드에 의한 인증 방식을 갖는 경우가 있다.

4. SSO 설계

위 3장에서 정의된 SSO 모델을 바탕으로 멀티서버로 구성된 인트라넷 시스템을 중심으로 설계하였다. 요구사항으로 시스템 연동 문제를 해결하기 위하여 사용자 관리를 통합관리하도록 사용자 변경 사항의 적용이 실시간으로 이루어져야 하고, CA서버 등 인증시스템은 기존 인프라를 이용하도록 하였다. 또한 각 시스템 별로 인증이 이루어진 후에도 시스템 별로 필요한 자료를 통신상에 적용할 때 인증서 기반의 보안을 적용하였다. 시스템 관리 관련 사항으로는 SSO 관리를 위한 관리자의 부담을 최소화하며 시스템 확장이 용이하도록 하였다. 또한 사용자의 추가, 삭제, 변경이 모든 시스템에 적용되도록 하며 예외 상태에 대한 조치가 용이하도록 하였다. 4장에서는 SSO 모듈의 기능과 연동을 위한 인사 데이타와 LDAP 데이타 구성에 관련된 부분을 설명한다.

4.1 SSO 모듈 설계

웹브라우저의 제한된 기술적 문제로 클라이언트와 서버 플랫폼 환경에 독립적으로 PKI 기반의 통신을 대행

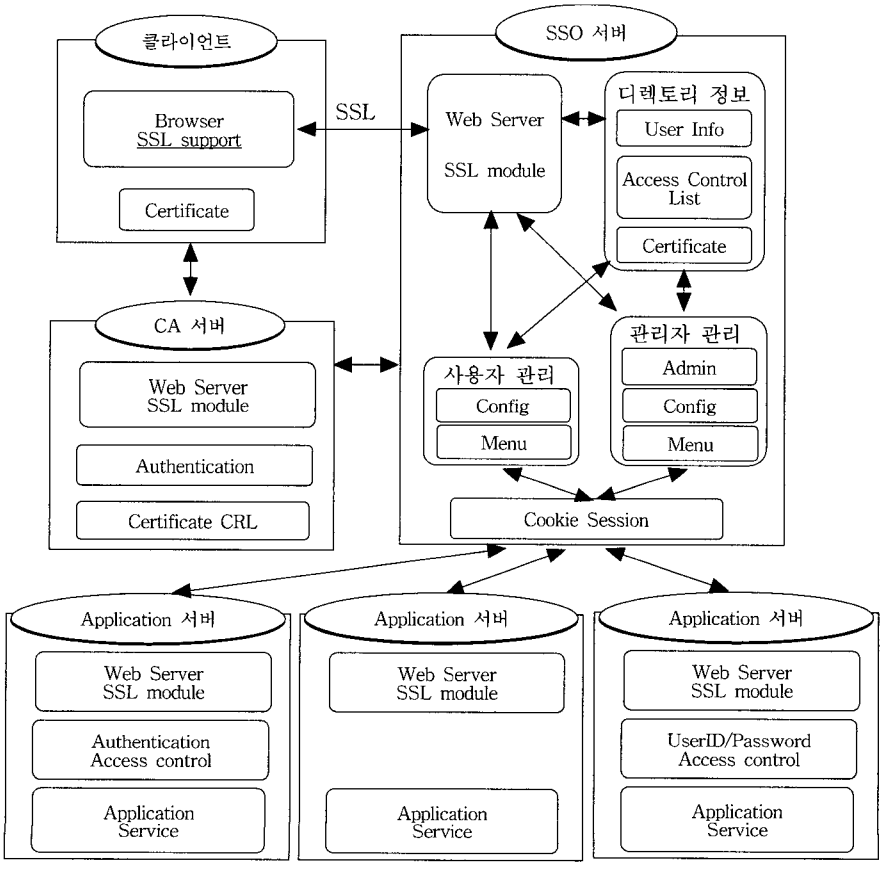


그림 5 SSO 모듈 구성

표 1 SSO 주요모듈 처리내용 및 기능

모듈	처리내용 및 기능	비고
SSO Server	- 인증서 기반 통신으로 사용자 및 서버 인증 - 인증된 사용자의 토큰 발행 - 사용자 및 리소스 설정 관리 - Client Agent와 암복호화 통신 - 다수의 Client Agent와 통신을 위한 로드 밸런싱 - SSO Server 로그 출력 - 서비스 접속 허용치 관리	관리 자용
Server Agent	- 토큰 인지 및 처리 - 클라이언트와 옵션에 따른 암복호화 통신 - 사용자 인증 확인 - 암호화방식 선택 - 다수의 Client Agent와의 통신을 위한 로드밸런싱 - Server Agent 로그출력	관리 자용
Client Agent	- 사용자 인터페이스 제공 - 서버 Agent와 옵션에 따른 암복호화 통신(선택) - 인증정보 유지를 위한 토큰 수령 및 전달 - Server Agent 상태 및 로그 출력	사용 자용
Applet	- 사용자의 인증서를 확인하여 클라이언트에 필요한 파일다운로드 - 클라이언트 구동	사용 자용
SSO RA	- CA 인증서 발급 준칙과 초기 사용자 설정 정책에 따라 개발	관리 자용
암복호화 API 적용	- CA에서 제공하는 API 적용	개발 자용

하기 위하여 Agent 방식의 기술 구조를 적용하였고, 클라이언트 Agent는 웹브라우저를 사용하면서 백그라운드로 실행된다. 기능에 따라 주요 모듈 처리 내용을 정리하면 표 1과 같다.

4.2 인사 데이타 연동 설계

인트라넷 운용상의 인증 관련하여 사내 조직원 여부를 판단하는 기준을 정할 필요가 있다. 이러한 조직 정보의 초기 데이타 및 변동 데이타를 효과적으로 구축, 반영하기 위하여 기존의 인사 DB와의 연동이 요구되며,

표 2 사원정보

필드명	설 명	연동필드	비 고
emp_no	사번(학번)	user	
emp_nm	이름	cn(LDAP),name(DB)	
dept_cd	부서(학과)	dept_id	
agency_cd	기관(대학)		
level_cd	직위코드	pos_id	
class_cd	직급코드	rank_id	
repl_dt	수정일		update 유무결정
status_cd	재직구분	status	
position_nm	소속명		
class_nm	직급명		
level_nm	직위명		

인사 DB 테이블 중 인트라넷에서 필요한 데이타를 정의하여 연동에 필요한 필수 요소만을 효과적으로 추출하도록 하였다. 연동 데이타로는 조직정보, 사원정보, 직급정보, 직위정보 등이 필요하며 표 2는 그 중에 사원정보 데이타만을 나타낸 것이다. 표 2에서 emp_no, dept_cd, agency_cd, level_cd, class_cd 등은 다른 필등에 비하여 더 중요하고 특히 emp_no는 Primary Key로서 적용된다. 사원정보는 인증서 발급시에 사내 직원인지 확인하는 과정과 SSO 서버에서 토큰을 발생할 때 조회 자료로 활용된다.

4.3 LDAP 정보 설계

초기 데이타 구축시엔 기존의 인사DB에서 인사정보 중의 일부를 가져와 LDAP에 사원정보를 반영하고, 이후에는 인사DB의 사원정보 변경시 LDAP에 자동반영한다. LDAP의 Object별 DN 및 속성(Attribute)을 구성함에 있어 필요한 DN 요소는 OU(Organizational Unit), 서버정보, 도메인정보, 부서정보, 사용자정보, 그룹정보, 직위정보 등으로 분류할 수 있으며 표 3과 같이 설계하였다. 또한 SSO 서버에 접근제어 정보로서 입력되는 정보는 표 4와 같이 사용자 속성정보를 정의하여 입력한다. 표 3과 4의 예에서와 같은 정보들은 인증서와 함께 LDAP서버에서 저장되어 서비스될 때에 응용시스템에서 접근권한을 제어할 수 있다.

표 3 Object Unit

Object Class	Organization Unit
DN	ou=x, o=Korea Telecom, c=KR
속성	**ou: server, domain, dept, user, group, position**

표 4 OU에서 사용자 속성 정보

Object Class	Person	
DN	user_id=x, ou=user, o=Korea Telecom, c=KR	
속성	**user_id: 사용자ID**	recv_send_f: 수발신 담당자여부
	sv_id: 서버ID	**login_passwd: 사용자 로그인 암호**
	name: 사용자 이름	passwd_chk: 사용자 결재 암호
	alias: 별명	passwd_chk_f: 결재시 암호확인 여부
	dept_id: 부서ID	method_how: 결재방법
	dept_name: 부서이름	mail_noty_f: 메일수신 알림 여부
	pos_id: 직위ID	board_noty_f: 게시물 알림 여부
	user_num: 사번	**signature: 메일 signature**
	sec_level: 보안등급	smtp: 메일서버

위의 표 3과 4에서와 같이 DN을 구성함에 있어 서비스를 추가하게 되면 LDAP 정보들을 확대할 필요가 있다. 본 논문에서 설계한 시스템은 인트라넷용 업무전산, 전자도서관, 특허정보 등 다양한 서비스의 분산된 시스템을 단일 인증을 통하여 서비스 받을 수 있도록 하였으며, 경영정보, 인사시스템, 재무/물자 등 사내 직원들을 고려한 웹용 시스템에서도 DN과 속성정보를 확장 정의하여 활용할 수 있도록 하였다.

4.4 인증서에 의한 시스템 활용

사용자는 모든 인트라넷 접속시 유효한 본인의 인증서를 SSO 서버에 전송함으로써 서버로부터 접근권한을 얻고, 전송된 인증서 내용을 키로 LDAP에서 사원정보를 추출한다. 이때 사원임이 확인되면 서버 도큐먼트 접근권한을 부여받고 LDAP에 접속한 사원정보 추출기능으로 현재 사용중인 사용자를 관리한다. 멀티서버로 구성된 인트라넷 서버간에 분산된 사용자들이 해당 서버로 자동 로그인 하는 서비스는 sv_id, name, port, ip_addr 등의 속성항목에 각 서버의 정보를 지정하고, domain_id, name, sv_id, topdept_id 등의 속성항목 중에 topdept_id에 부서정보를 지정하면 사용자는 자기가 속한 인트라넷 서버로 자동 분기된다. 부서, 사용자, 그룹, 직위 정보와 사용자 정보에서 각 응용서비스에 대한 속성을 추가한다. 이와 같이 SSO 서버의 응용프로그램들에 대한 정보를 부가함으로써 서버 상에서 통합메뉴 형태를 구성하여 사용자가 원하는 응용서비스를 사용할 수 있다. 그림 6은 멀티서버로 구성된 각각의 응용시스템을 통합메뉴로 묶어 SSO를 적용한 것으로서 현재는 인증서 발급 및 폐기 등 관리에 대한 사용자들에게 익숙하지 않아서 ID/Password 기반에 의한 서비스를 제공하고 있으며, 인증서 발급을 제외하고는 사용자들이 사용하는 방법이 유사하다.

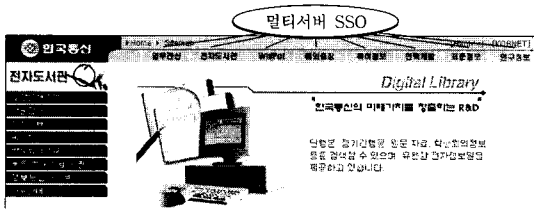


그림 6 SSO 적용 시스템

4.5 결과 분석

인증서를 발급하는 기관이 국가에서 공인된 법인이고 인증서 발급시에 비용이 발생하며, 주기적으로 재발급을 하여야 하기 때문에 단위 기관내에서만 사용하는 인트라넷은 사설 CA를 설치하여 사용하는 경우도 있다. 본 연구에서는 사설 CA를 이용하여 인증서 기반의 SSO 파일럿 시스템을 구성하였다. 인증서 방식의 SSO 메커니즘 표준이 정해져 있지 않은 상황에서 구현 모델은 디렉토리 서버를 사용자 접근제어 정보의 창구로서 제공하고, 각 응용프로그램의 서버가 요청한 조건의 결과를 처리하는 방식이기 때문에 부하를 고려하여 설계에 반영하였다. PKI에 의한 인증서 기반의 SSO는 SPUR이나 ID/Password의 패스워드 동기화에 의한 보안성이 뛰어나고, 인증서 발급에 대한 표준화 및 전문 서비스 기관이 있으며, LDAP을 활용한 사용자 정보관리 등이 용이하여 전사적인 또는 전 가입자에 대한 통합관리를 제공할 수 있다. 특히 본 연구에서는 인사 데이타와 LDAP의 DN을 활용하여 차세대 접근 통합권한관리 기술인 PMI 개념인 사용자 접근권한 부분까지 일부 적용하였다.

인증서 기반의 타 SSO 시스템들과의 비교사항으로는 인증서를 사용하는 부분은 같지만 클라이언트와 서버간의 통신 및 각 Agent의 역할 등에 대해서 조금씩의 차이를 두고 있고, 각 SSO시스템들의 설계에 대한 구조적 메커니즘이 제시된 것이 없기 때문에 본 연구에서는 이들간의 비교를 하지는 않았다. 본 연구에서는 각 SSO 모델에 대한 분석을 표 5와 같이 나타내었다.

표 5 SSO 모델 분석

SSO 모델	장 점	단 점
SPUR	- 고도 기술이 필요치 않음 - 제도적/강제적으로 처리 - 투입비용 낮음	- 보안성 취약 - 다양한 서비스 수용 곤란 - 기존 시스템 통합 곤란 - 전산환경 변화 대응 미약
패스워드 동기화	- 개발 방법 다양 - 개발자 융통성 - 사용 방법 용이	- 보안성 취약 - 시스템간 동기화 메커니즘 및 안정성 유지 어려움 - 표준 무, 개발기간 소요
인증서 방식	- 보안성 강화 - 컴포넌트 형태로 API에 의한 개발 기간 단축 - 구성요소별 표준 - SmartCard 등 인증수단 다양화	- 인증서 신청 폐기 등 처음 사용시 어려움 - 구성요소별 투입비용 높음
SSO 구현 모델	- 전사적인 웹통합 환경 - 데이타 및 통신상에서 보안강화 - LDAP, CA 인터넷 표준 적용 - LDAP 서버로 접근 통합 - Config, Session 유지 등	- 인증서 방식과 동일

SSO를 적용한 시스템들의 응용서비스가 무엇인가에 따라 인증서를 적용하는 것에 대한 견해가 확연히 다를 수 있다. 현재 사이버뱅크에서는 공개키 인증서를 배제하고서는 다른 적용할만한 대체 기술이 없기 때문에 광범위하게 적용되고 있으며, 적용 시스템과 응용서비스가 증가되면서 SSO에 대한 관심이 높아지고 있다. 그러나 그림 6과 같이 사내 인트라넷 에 대한 사용자들의 반응은 잘못된 결과가 있더라도 비용상의 문제점이 발생하지 않는다는 생각과 인증서 발급 등의 절차에 불편을 제시하기 때문에 인증서 기반의 SSO 확대 적용에는 발전된 인증서 관리모델이 제시되고, 사용자들이 수긍하고 사용할 수 있도록 정보의 질을 높여갈 필요가 있다.

5. 결 론

시스템마다 별개로 수행되었던 사용자 계정의 등록/수정/삭제 작업과 권한설정, 접근제어 설정작업을 중앙에서 한번에 수행할 수 있으며, 모든 사용자 정보가 중앙에 통합됨으로써 시스템 사이의 정보 불일치를 피할 수 있는 인증서 기반의 SSO를 연구하였다. 본 연구에서는 인트라넷 분산서버에 중점을 두어 SSO를 구현하였으나 이종 멀티서버 환경에서 LDAP의 DN과 속성을 필요에 따라 확장 정의하여 사용자 접근 로직을 통합하는 부분과 X.509 4th Edition 포맷에서 제시하는 PKI와 PMI의 통합 인증서 포맷에 대한 연구를 지속할 계획이다.

e-Business를 위한 전자상거래 Portal 사이트들도 이제까지의 불완전한 인증체계를 과감히 인증서 기반의 SSO로 전환해서 서비스해야 할 것이며, 사업적용 모델이 인터넷을 기반으로한 B2B, B2C 형태의 서비스에 해당되는 물류, EDI, 전자조달, 전자상거래, 금융, 보험 등과 같은 서비스에서 더욱 인증서 기반의 SSO 서비스가 확대 적용될 것으로 기대된다.

참 고 문 헌

[1] Netscape manual, "Single Sign-On Deployment Guide," http://developer.netscape.com/docs/manuals/security/SSO/index.htm

[2] White Paper, "Single Sign-On in Windows2000 Networks," http://www.microsoft.com/TechNet/win2000/win2ksrv/prodfact/nt2ksso.asp

[3] White Paper, "Password Synchronization and Single Sign-On Between Multiple Platform," Microsoft.

[4] White Paper, "Windows 2000 Kerberos Interoperability," Microsoft.

[5] X/Open Single Sign-on Service(XSSO)-Pluggable Authentication Modules, The Open Group, 1997.

[6] 고승철, 이상진, "키분배와 인증기법", pp457-459, 전자공학회지 제21권 제5호, 1994.

[7] 오창석, 데이타 통신, pp233-282, 영한출판사, 1999.

[8] 이임영, 송유진, 현대암호, pp109-134, 생능출판사, 1999.

[9] 김지연, "PKI 구성객체의 상호연동을 위한 명세서 분석", 한국정보보호센터, 1998

[10] Netscape manual, "Introduction to Public-Key Cryptography," http://developer.netscape.com/docs/manuals/security/pkin/index.htm

[11] White Paper, "Windows 2000 Public Key Interoperability," Microsoft.

[12] 김기현, "접근통제기술 개요", http://www.kisa.or.kr/technology/sub3/AC_9901.html

[13] Netscape manual, "Access Control Programmer's Guide," http://developer.netscape.com/docs/manuals/enterprise/accessapi/contents.htm

연 승 호

1985년 충북대학교 공대 컴퓨터공학과 학사. 1988년 충북대학교 대학원 컴퓨터공학과 석사. 2000년 충북대학교 대학원 컴퓨터공학과 박사. 1988년 7월 ~ 1990년 10월 LG전자 가전연구소 연구원. 1990년 11월 ~ 현재 한국통신 멀티미디어연구소 선임연구원. 관심분야는 정보보호 플랫폼(ESM, EAM), 영상처리

박 현 규

1996년 연세대학교 전기공학과 학사. 1998년 연세대학교 전기공학과 석사. 1999년 ~ 한국통신 멀티미디어연구소 전임연구원. 관심분야는 정보보호(PKI, PMI), MPEG, 디지털 신호처리

오 희 수

1983년 광운대학교 전자계산학과 학사. 1987년 서울대학교 컴퓨터공학과 석사. 1990년 11월 ~ 현재 한국통신 멀티미디어연구소 근무중. 관심분야는 정보보호(SSO, PKI, PMI)

김 영 헌

1981년 부산대학교 전기기계공학과 학사. 1983년 KAIST 전기및전자공학과 석사. 1983년 3월 ~ 현재 한국통신 멀티미디어연구소 정보보호연구실장 선임연구원. 관심분야는 EAM, ESM, 정보보호 컨설팅 등

전 병 민

1976년 한국항공대학교 전자공학과 졸업. 1978년 연세대학교 전자공학과 석사. 1988년 연세대학교 컴퓨터공학과 박사. 1978년 ~ 1982년 공군사관학교 전자공학과 전임강사. 1982년 ~ 1986년 동양공업전문대학 통신과 조교수. 1992년 ~ 1993년 미시간대학교 교환교수. 1986년 ~ 현재 충북대학교 컴퓨터공학과 교수. 1995년 ~ 현재 한국통신학회 평의원. 1998년 1월 ~ 1998년 12월 한국통신학회 학술이사. 1999년 ~ 현재 한국통신학회 충북지부 지부장. 2000년 ~ 현재 한국정보과학회 평의원. 관심분야는 패턴인식, 디지털 신호처리 및 영상처리