# 인증서 기반 사용자 인증 및 정보보호 서비스 솔루션

*Authentication & Information security Solution*

## 공개키 기반 구조 [ PKI ]

### PKI란

" 공개키 알고리즘을 통한 암호화 및 전자서명을 제공하는 복합적인 보안시스템 환경입니다.
즉, 암호화와 복호화키로 구성된 공개키를 이용하여 송수신 데이터를 암호화하고 디지털 인증서를 통해 사용자를 인증하는 시스템입니다."

### 인증기관

인증기관(CA, Certification Authority)은 사용자들에게 인증서를 발급하여 주는 기관입니다. 인증서의 발급 및 인증서의 추출, 폐기, 갱신, 교체에 이르는 라이프 사이클을 관리하며 고객의 요구에 따라 인증서 조회 기능을 제공합니다.

### 전자서명

전자서명(Digital Signature)는 공개키 암호 알고리즘에 기반하는 알고리즘입니다. 전자 서명을 공개키 암호 알고리즘의 암호화 사용 방법과 반대로 이루어집니다.
서명자는 자신의 개인키를 이용하여 서명하고, 상대방은 서명자의 공개키를 이용하여 서명을 검증할 수 있습니다.

## SSL [ Secure Sockets Layer ] / TLS

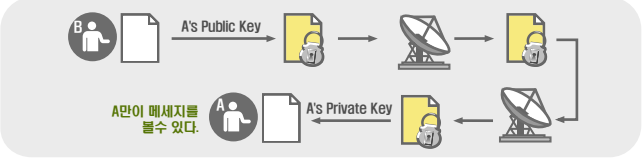
SSL은 TCP와 어플리케이션 계층 사이에 존재하는 Presentation 계층 서비스로 플랫폼, 어플리케이션과 독립적입니다.
SSL은 클라이언트/서버 사이의 안전한 통신 채널관리를 담당하며 이들 사이에 전달 되는 데이터를 암호화기능을 제공합니다.

### 목적

SSL의 목적은 전자상거래와 같이 보안에 민감한 정보에 대한 트랜잭션처리입니다. 처리되는 트랜잭션의 중요도와 가치에 따라 일부 혹은 전부를 이용하게 됩니다.

#### 기밀성 (Encrypt)

네트워크로 전달되는 정보가 비 인가된 사용자의 불법적인 행위 및 처리 등으로 인하여 내용이 유출되는 것을 방지합니다.

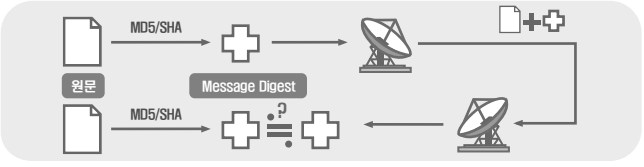



#### 신뢰성 (CA / Certificate Chain)

클라이언트 및 서버는 공인 인증기관에서 발행된 인증서를 통하여 서로의 신원을 확인할 수 있습니다.

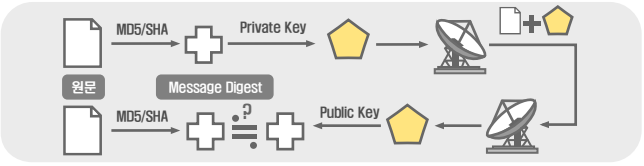
#### 무결성 (Message Digest)

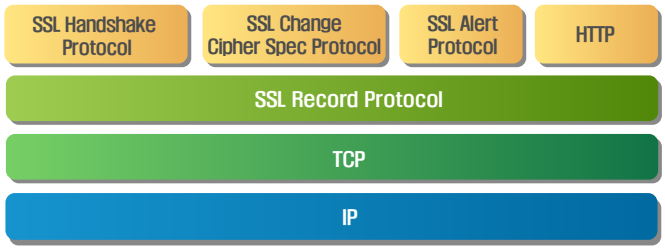
데이터의 내용이 비 인가된 방식에 의해 변경 및 삭제되는 것을 방지합니다.




#### 부인방지 (전자서명)

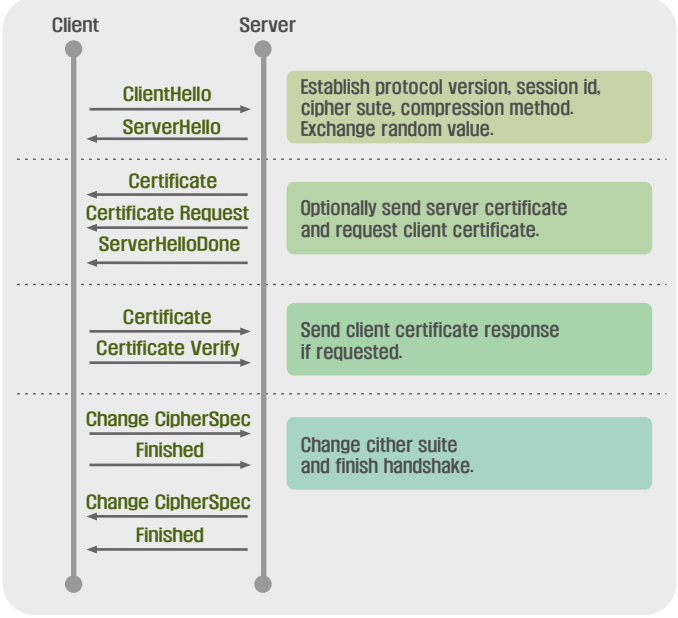
정보보안의 방법에 의해 데이터의 발신자가 발신 사실에 대한 부인을 방지합니다.




### SSL Handshaking

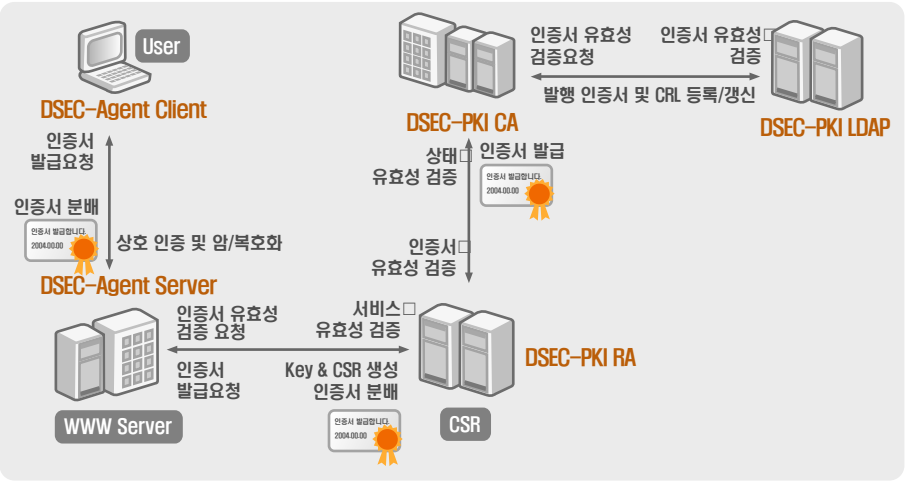
SSL handshake 프로토콜은 SSL 세션을 최초 시작할 때, 클라이언트와 서버간에 안전한 연계의 수립을 위하여 클라이언트와 서버간의 상호 인증을 수행하고 암호 메카니즘등의 정보를 교환하며, SSL record 프로토콜에서 사용할 수 있는 세션키를 생성하는 과정등을 정의 합니다.



## 인증서 기반 정보보호 서비스

인터넷 및 E-Biz환경에서 사용자 인증 및 정보보호기능을 제공하기 위해 기반이 되는 핵심솔루션을 구현한 것입니다. □
다양한 사용자 환경 중 현재 가장 사용도가 높은 Web환경에서 사용자 인증을 위한 PKI 솔루션입니다. PKI 기반 솔루션 및 요소 기술인 ActiveX컨트롤, JSP, CGI구현 기술을 활용하여 안정적인 Web client – Server Agent 구조 입니다.

### 시스템 구성도

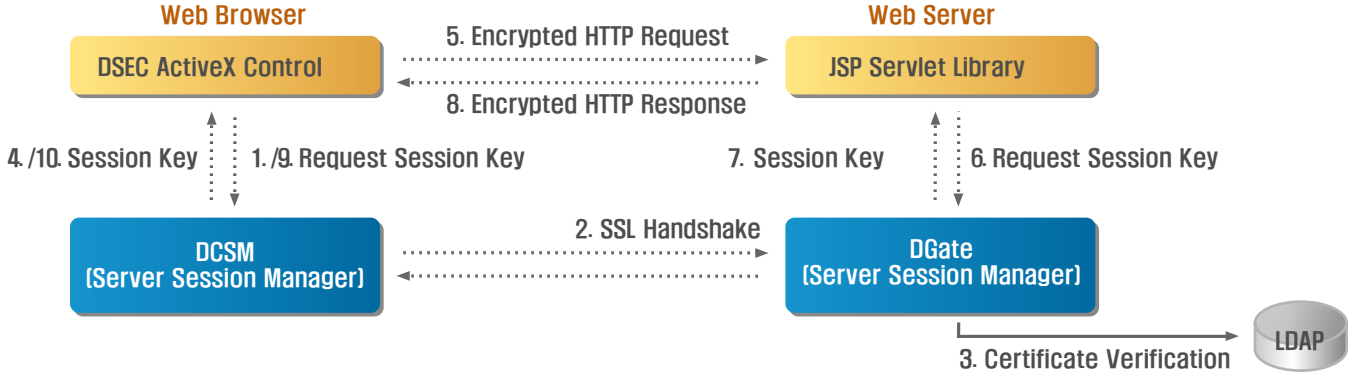



전체 시스템은 DSEC-PKI(CA/RA/LDAP) Server 부분과 DSEC-Agent(Client/Server) 부분으로 구성 되어있습니다. 사용자 인증 및 정보보호/보완 의 요소인 송수신 정보의 내용이 제3자에게 노출되지 않는 기능인 정보 기밀성(confidentiality/secrecy)과 사용자의 신분 및 행위를 증명하는 인증(authentication), 교환되는 정보가 전달되는 과정에서 변조되었는지의 여부 판단하는 무결성(integrity) 그리고 부인방지(non-repudiation)의 요소를 기반으로 합니다.

DSEC-PKI부분은 인증서에 기반한 사용자 인증 및 전자서명, 데이 암호화를 통한 안전한 서비스의 보장과, 공개키/비공개키 생성과 인증서 관리(발급/등록/폐기/유효성검증) 자체개발 운용 프로토콜을 적용하고 있습니다.

DSEC-Agent부분은 다양한 웹 기반 서비스의 제공과 RAS 1024-bit기반 사용자 인증 및 전자서명 지원, 3DES 192-bit/SEED 128-bit 기반 데이터 암복호화 지원, 인증서 기반 인증 과 익명 기반 인증 지원, 전체 암호화 부분과 부분 암호화를 지원하고 있습니다.

## 전체 시스템 구성도




## 클라이언트 모듈

### ActiveX

사용자가 이용하는 User Interface입니다. 사용자는 자신의 인증서를 관리하며, UI를 통해 인증서의 요청, 폐기들을 요청할 수 있습니다. 또한 기본 서비스(금융서비스 등)을 이용할 수있으며, 통신은 보안모듈을 이용한 인증서 기반 비밀통신을 합니다.

- 로그인, 인증서 요청
- 사용자 인증서 설치
- 로컬 저장소 인증서 관리
- 인증서 해지 목록 관리
- 암호/복호를 이용한 보안 통신

### DSEC 보안 모듈□

보안에 관련된 암호화 알고리즘 및 해쉬 알고리즘등이 구현된 라이브러리 □ 모듈입니다. 암복호화 및 데이터 무결성등을 검증합니다. 서버에 지원하는 암호 알고리즘등을 선택할 수 있도록 다양한 알고리즘을 제공합니다.
구현 언어는 c/c++ 언어입니다.

### DCSM

현재 사용자의 보안 통신을 위한 세션을 관리하며, SSL Handshaking을 이용하여 클라이언트와 서버간에 연결 상태를 관리합니다

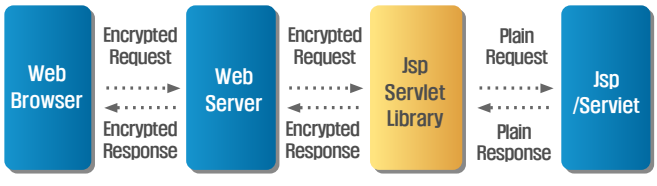
## 서버 모듈

### DGate

현재 웹서버에 접속한 클라이언트 사용자들의 세션 및 세션생성시 발생하는□ 키를 관리합니다. □
웹서버 – 클라이언트간 통신시 암/복호화 시 이용되는 키를 제공합니다.

### JSP/Servelt 라이브러리

암/복호화에 필요한 부가적인 기능을 수행하는 자바 서블릿 라이브러리로 기존 JSP/Servlet 표준 인터페이스의 wrapper 클래스로 구현됩니다.
응용 개발자는 암복호화와 관련된 사항을 고려하지않고도 편리하게 PKI 시스템이 제공하는 기능을 사용하여 웹 응용프로그램을 작성할 수 있도록 합니다.





Nehom

회 사 명 : 내홈닷컴
전화번호 : 1566-6346
FAX 번호 : 02) 6008-3876

홈페이지 : http://www.nehom.com
주 소 : 443-400 경기도 수원시 영통구 망포동 558번지 LG 탑프라자 5층
연 구 소 : 305-350 대전시 유성구 가정도 34번지 #105