유넷시스템

TrustNET 제품소개서

Advance Edition (Clientless)

2020.09

TrustNET

목차

1. TrustNET 소개

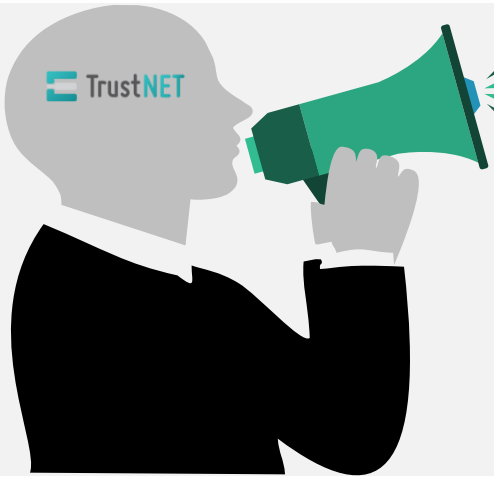
가. 제안 배경
나. 관련 표준
다. 제품 구성
라. 운영 환경

가.제안배경

PKI 개요

Public Key Infrastructure

전자상거래 시스템과 같은 정보시스템에 안전성을 부여하며,
네트워크 상에 연결된 사용자와 메시지에 대한 인증기능을
부여하기 위한 공개키 방식을 이용한 전자인증기반 기술 체계.



암호화 신뢰성 확보
거래정보 암호화를 통한 정보보호

인증서 사용자 인증
거래 행위자의 신원확인

자료인증 자료의 무결성 보증
거래정보의 위/변조 방지

전자서명 거래사실 부인 방지
전자서명을 통한 거래 신뢰성 확보

별도의 클라이언트용 프로그램 설치 없이 공개키 방식의 인증서 발급 가능

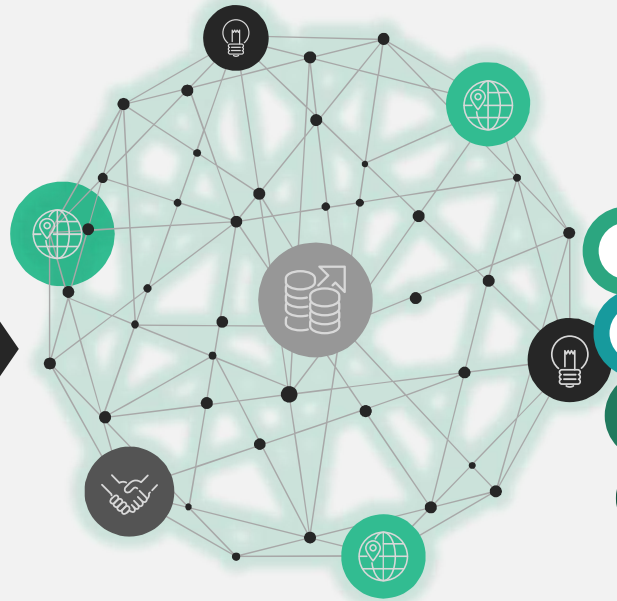
가.제안배경

Needs

분산 시스템 환경에서의 데이터 교류를 통한 비즈니스 활성화에 따라 정보보호의 필요성이 대두되고,
다양한 통신 환경 및 단말기를 통한 정보 교류는 언제나 정보유출의 위험성을 내포하고 있음
안전한 정보교류를 통한 비즈니스 활성화를 위해 데이터 무결성 및 기밀성이 보장되어야 하고 확장성을 용이하게 할 수 있는 보안 인프라가 필요함

배 경
인터넷발전,
인터넷을 통한 개인신상정보,
기업 정보자산의 유통정보 증가

문제점
통신내용도청,
불법사용자데이터변조,
송수신사실 부인



- 기밀성(Confidentiality)
- 무결성(Integrity)
- 인증(Authentication)
- 부인방지(Non-repudiation)

TrustNET
Public Key
Infrastructure

나.관련표준

인증기관 적용 표준

기술요소	표준안 근거	기술설명
인증서 규격	X.509 v3, RFC3280	적용된 기술은 인터넷 표준안인 RFC 2459 의 인증서 규격을 채택하여 다른 PKI 영역과의 연동을 위한 최소한의 기능을 갖춤
인증서 폐기목록규격	X.509 v2, RFC3280	인증서와 같이 인터넷 표준안인 RFC 2459 가 적용되어 업체간 연동을 갖춤
인증서 관리절차	RFC 2510, RFC 2511 draft-ietf-pkix-cmp-transport-protocols-01	인증서 발급/폐기/갱신을 위한 상호 메시지 부분에서 인터넷 표준안인 RFC 2510과 실제 메시지의 전송부분의 인터넷 표준안인 draft-ietf-pkix-cmp-transport-protocols-01 를 적용하여 종단간 연동성을 갖춤
인증서 검증	RFC 3280	인증서의 유효성 검증을 위한 경로인증부분은 인터넷 표준안인 RFC 2459를 준용하여 상호 인증 시에 인증서의 검증에 대한 연동성을 갖춤
인증서 분배	RFC 2559, RFC 2585, RFC2587	발급된 인증서를 배분하기 위해 표준화된 디렉토리 구조를 통한 LDAP 지원 및 HTTP 나 FTP 기타 네트워크 프로토콜을 통한 접근자를 위해 RFC 2585를 적용하여 분배 편의를 도모함

나.관련표준

통신 프로토콜 표준

기술요소	설 명	표준안 근거
CRMF	Certificate Request	RFC 2511
CMP	Internal messaging cross certification	RFC 2510
SSL	Secure Socket Layer	RFC 6101
X.509 PKI-OCSP	Online Certificate Status Protocol	RFC 2560
CMS	Cryptographic Message Syntax	RFC 2630
LDAP	Communication LDAP	LDAP
SQL	Internal Communication	SQL
HTML5	HTML5	World Wide Web Consortium

나.관련표준

기술표준

기술요소	설 명	표준안 근거
RSA 암호화	PKCS #1	RSA 알고리즘을 이용한 데이터 암호화 및 전자서명 생성과 관련된 업계 표준을 지원
패스워드 기반 데이터 암호화	PKCS #5 v2.0	패스워드 기반의 암호화를 위한 키 유도 함수 PBKDF2 및 8바이트 이상의 블록 암호 키를 이용한 PBES2 를 지원
인증서 확장 구조	PKCS #6	확장된 인증서 구조를 지원하기 위한 업계 표준으로 서명 메시지 등에서 첨부 기능 지원
전자서명 및 암호데이터	PKCS #7, RFC 2630, RFC 2634	공개키 암호화 방식을 이용해 전자서명 메시지 및 암호메시지, 다이제스트 메시지 등의 전자문서 표준을 지원
개인키 구조	PKCS #8	개인키의 보관 및 이동을 위한 메시지 형식 및 암호화된 개인키 표준을 지원
인증서 요구 양식	PKCS #10, RFC 2511	인증서 발급 요구서 메시지의 표준 구조로 PKCS #10 에 비해 POP 및 구조가 개선된 RFC 2511 추가 지원
사용자 정보 교환	PKCS #12	사용자 개인키 및 인증서 기타 보안자료들의 이동 보관 및 전달 양식 표준으로 PC 에서의 인증서 이동수단을 위해 지원

다.제품구성

제품구성 및 주요기능(1/2)

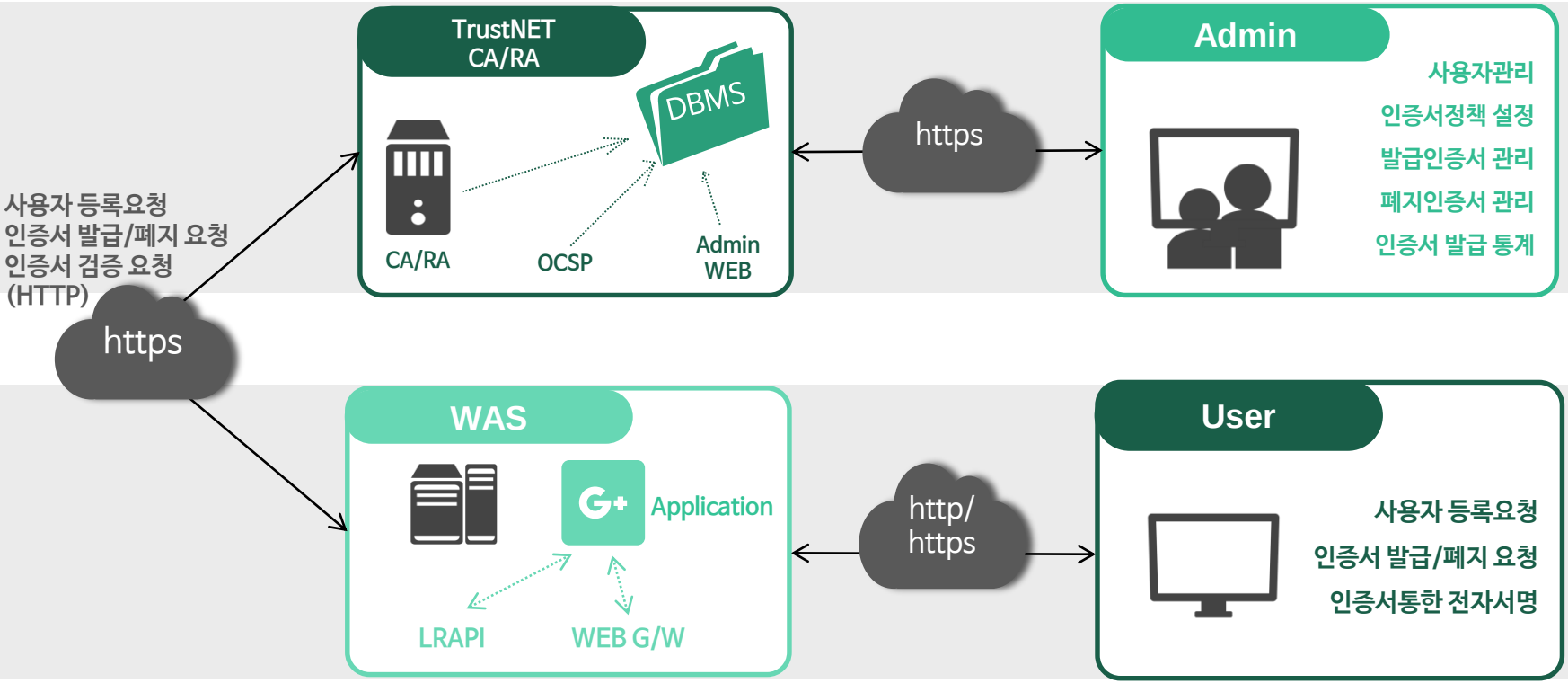
제품구분			기 능	비 고
서버	TrustNET CA/RA		사용자정보의 등록 및 인증서의 생성, 폐지, 효력정지 기능을 수행하는 PKI 핵심 시스템	- TrustNET 에서는 인증서 유효성 검증을 OCSP 를 기본으로 함 - CA, OCSP 서버가 핸들링하는 RDB 별도 필요 - CRL 사용 시 LDAP 별도 필요
	TrustNET OCSP		실시간으로 인증서 유효성을 검증하는 시스템	
	관리자 Web Console		인증서 정책 설정, 발급, 폐기 및 통계 정보 확인	
응용	TrustNET LRAPI, Web Gateway	ActiveX client	TrustNET CA/RA 서버에 인증서 발급을 위해 사용자 등록, 사용자 삭제, 인증서 폐지 기능 수행을 위한 라이브러리	TrustNET CA client 가 설치되어 있어야 함
클라이언트	TrustNET CA-Client For PC	ActiveX client	사용자 PC에 설치되는 컨트롤로 Windows IE 환경에서 인증서 발급 및 관리를 수행	
		Multi client	사용자 PC에 설치되는 컨트롤로 Windows, Linux, Mac 환경에서 인증서 발급 및 관리를 수행	Non Plug-in Client 사용 (Windows IE는 Active X를 사용하기도 함)
	TrustNET CA-Client For Mobile	Internal Storage	내부 저장소에 인증서, 개인키를 저장하며 Application 형태로 제공되며 VPN App 또는 해당 인증서가 필요한 다른 App 에서 인증서 사용 가능	Android, iOS 환경 지원
		External Storage	외부 저장소에 인증서, 개인키를 저장하며 Library 형태로 제공되며 인증서 발급 및 관리를 수행	Android, iOS 환경 지원
	TrustNET Non-Native CA-Client		별도의 클라이언트 모듈 설치 없이 웹에서 클라이언트 기능 수행	HTML5를 지원하는 모든 웹브라우저

제품구성 및 주요기능(2/2)

제품구분		기 능
Toolkit	TrustNET Toolkit for JAVA	C/S Application 운영 환경에 적용하는 보안 라이브러리
	TrustNET Toolkit for C/S	자바통합환경에 적용하는 보안 자바 클래스
	TrustNET Toolkit for ASP	NT용 ASP 웹서버 환경에 적용하는 보안 라이브러리
	TrustNET Toolkit for .NET	.NET Application 환경에 적용하는 보안 라이브러리
	TrustNET Toolkit for PHP	PHP 기반의 웹 환경에 적용하는 보안 라이브러리

다.제품구성

구성개념도


TrustNET
CA/RA
DBMS
CA/RA
OCSP
Admin
WEB
https
Admin
사용자관리
인증서정책 설정
발급인증서 관리
폐지인증서 관리
인증서 발급 통계
사용자 등록요청
인증서 발급/폐지 요청
인증서 검증 요청
(HTTP)
https
WAS
Application
LRAPI
WEB G/W
http/
https
User
사용자 등록요청
인증서 발급/폐지 요청
인증서통한 전자서명

라.운영환경

지원 환경

제품구분			지원 환경
서버	TrustNET CA/RA TrustNET OCSP 관리자 Web Console		JAVA 1.7 이상의 모든 OS 환경 지원 DBMS : Oracle, MS-SQL, MySQL, MariaDB, TiberoDB 지원 (그 외 DBMS 는 포팅하여 지원 가능)
응용	TrustNET LRAPI, Web Gateway	ActiveX client	JAVA 1.3 이상의 모든 OS 환경 지원
클라이언트	TrustNET CA-Client For PC	ActiveX client	Browser : Internet Explorer OS : Windows (Windows 8.1 tile UI 제외)
		Multi client	Browser : Chrome, Safari, Opera, Firefox, Edge OS : Windows, Mac, Linux
	TrustNET CA-Client For Mobile	iOS	iOS 6.0 이상
		Android	Android 4.0 (Ice Cream Sandwich) 이상 (Internal Storage Version 기준)
	TrustNET JavaScript CA-Client		HTML5 를 지원하는 모든 OS및 웹브라우저 수정

2. TrustNET CA/RA

가. 제품 설명
나. 제품 기능

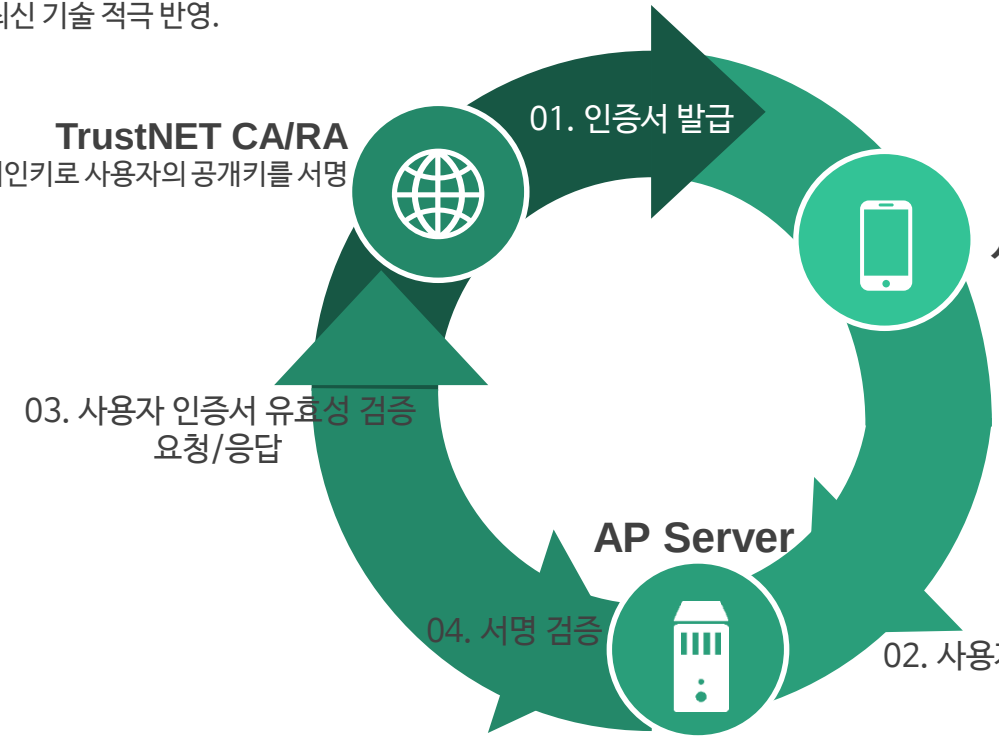
가.제품설명

PKI에서 핵심 역할에 해당하는 인증기관(Certificate Authority), 등록기관(Registration Authority) 시스템.

사용자의 정보 등록을 통해 사용자 DN을 부여하고 인증서 발급을 위한 참조번호, 인가코드를 발행.

인증서 발급, 폐지 기능을 수행하고 사용자 인증서를 조회하여 인증서 검증 수행.

국제 표준 기술 및 최신 기술 적극 반영.



나.제품기능

주요기능

인증서 관리 기능

모든 인증서의 발급, 재발급, 폐지 기능
RFC 2510 CMP 를 이용한 인증서 관리 기능
DBMS 종류에 상관없이 인증서 저장 관리 기능
(별도 DBMS 를 사용하지 않을 경우 MariaDB 사용)
LDAP 서버 연동을 통한 인증서 게시 기능

인증서 정책 설정 기능

인증서 유효기간, 키길이, 키사용에 대한 설정 기능
1인 1인증서 또는 1인 다 인증서 정책 설정 기능
인증서 보존 기간에 대한 설정 기능
CRL 갱신 주기 설정 기능

CRL 생성 및 관리 지원

인증서 유효성 검증을 위해 OCSP를 기본으로
제공하고 있으나 별도 요청에 의한 CRL 생성 및
LDAP 게시 기능 제공
CRL 갱신 주기 설정에 따라 주기적으로
갱신되며, CRL 게시 위치를 인증서에 첨부함

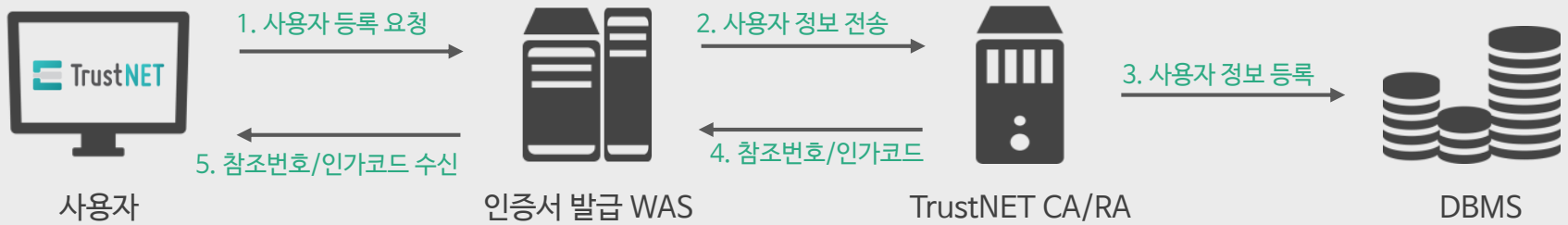
사용자 관리 및 통계

사용자를 구분하여 등록, 삭제 기능
인증서 정보(상태, SN, DN 등) 조회 및
퇴사 등으로 인한 인증서 폐지 기능 제공
월별 사용자 등록 통계 기능
월별 인증서 발급 및 폐지 통계 기능

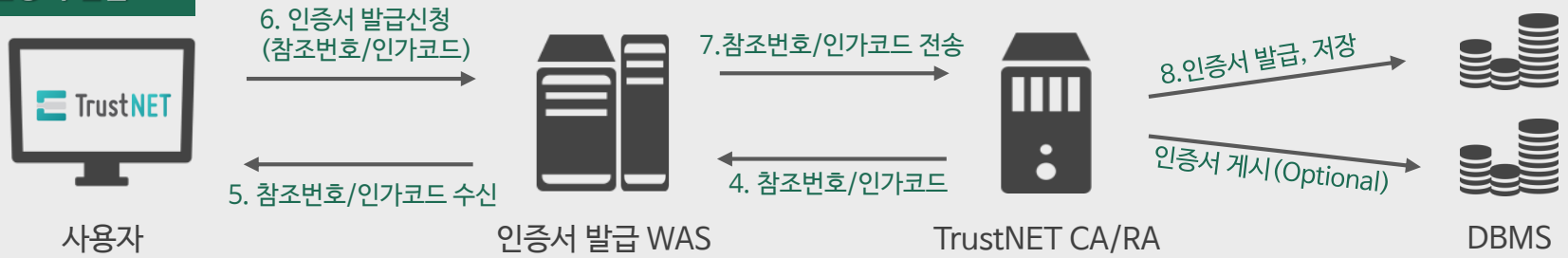
나.제품기능

인증서 발급 절차

사용자 등록



인증서 발급



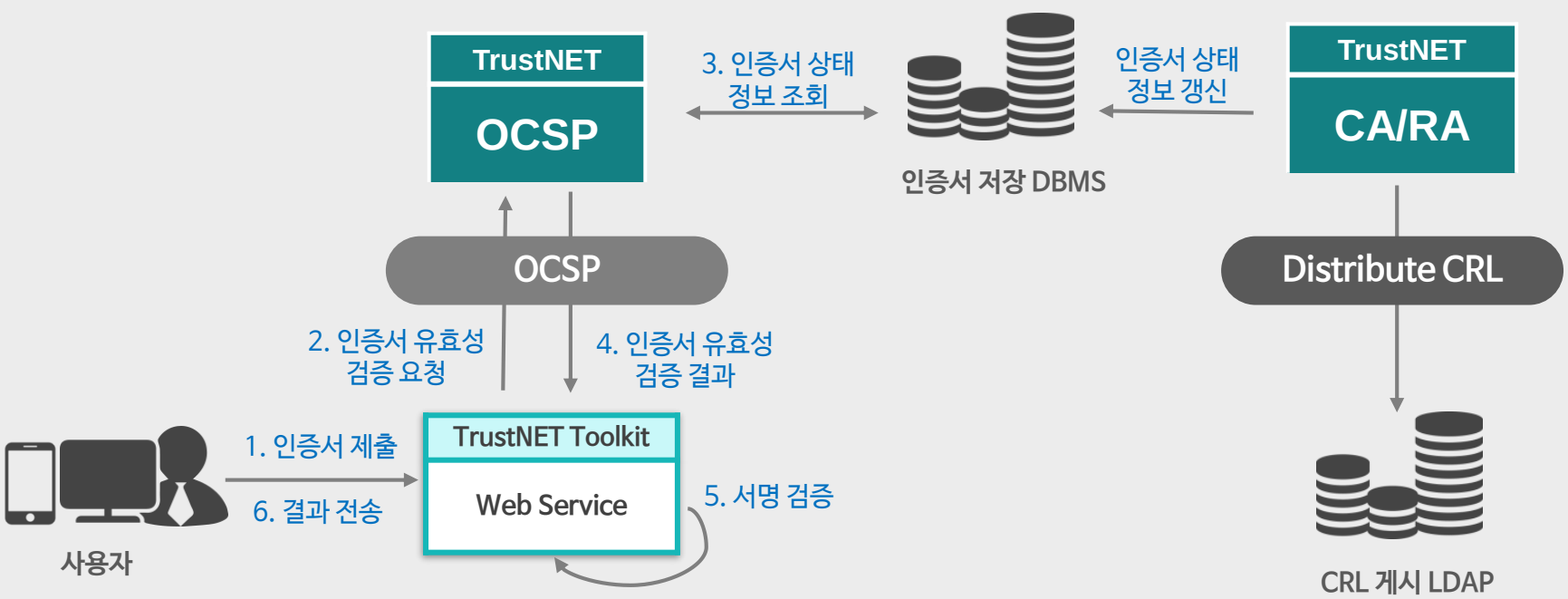
3. TrustNET OCSP

가. 제품 설명
나. 제품 기능

가.제품설명

제품설명

TrustNET OCSP는 CRL (인증서 폐기 리스트)요청 없이 인증서의 상태를 확인하기 위한 시스템으로
인증서의 유효성을 실시간으로 검증할 수 있는 시스템 , 고객사의 요청으로 LDAP 구성을 하여 CRL 검증을 할 수 있는 기능도 제공



나.제품기능

제품기능

인증서의 유효성을 실시간으로 검증 할 수 있는 시스템

실시간 인증서 상태 확인

- ✓ OCSP 검증 요청에 대하여 검증 요청 인증서를 실시간으로 상태를 확인하는 기능
- ✓ 폐기된 인증서에 대한 폐기 일시 및 폐기 사유 정보를 구할 수 있음
- ✓ 인증서 유효성 검증 실패에 대한 인증서의 실패 원인을 로그에 기록하는 기능

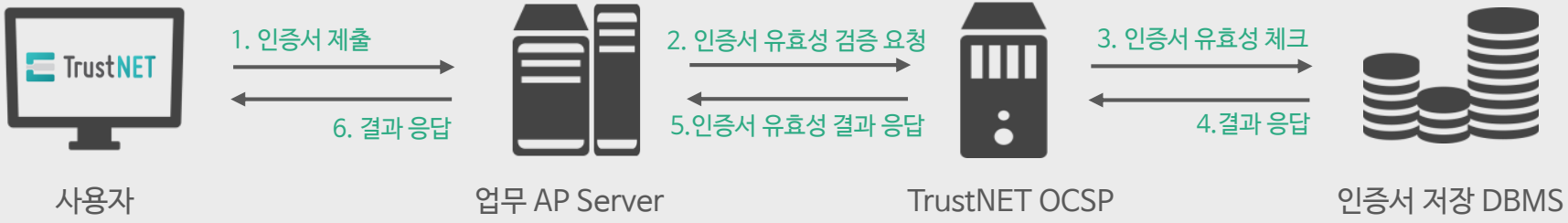
OCSP 정보 검증 기능

- ✓ OCSP 요청 정보 자체에 대한 서명 확인 기능
- ✓ OCSP 요청자의 인증서를 발급기관의 공개키로 검증하여 발급기관에서 서명한 인증서인지를 검증
- ✓ OCSP 요청자의 인증서가 유효한 인증서인지 발급기관 DB 정보와 비교해 발급자의 인증서가 종속된 인증기관의 인증서 인지 확인
- ✓ 검증할 인증서의 발급자 정보를 발급기관의 발급 인증서와 비교하여 발급기관에서 발급된 인증서인지를 검증하는 기능

나.제품기능

인증서 검증 절차

OCSP 검증



CRL 검증

4. TrustNET LRAPI, Web Gateway

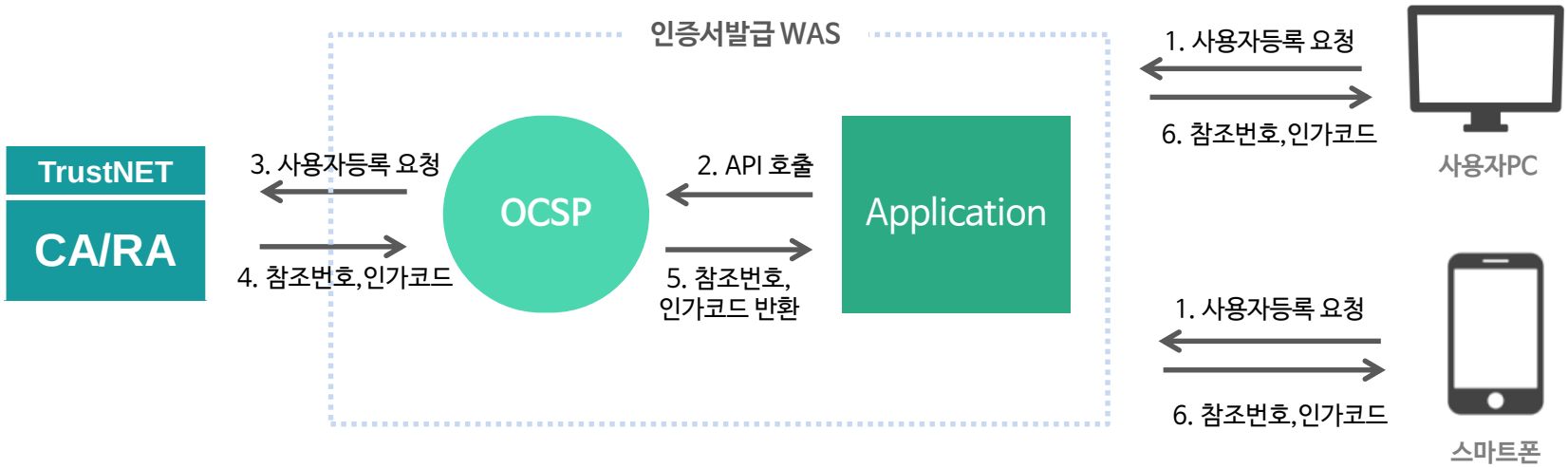
가. 제품 설명
나. 제품 기능

가.제품설명

LRAPI

TrustNET CA/RA 서버에 인증서 발급을 위해 사용자 등록, 사용자 삭제, 인증서 폐지의 기능 수행을 위한 API

라이브러리 형태의 제품이며, 인증서 발급을 위한 웹 화면 제작 시 응용프로그램에서 각 기능에 해당하는 API를 호출하여 사용



나.제품기능

제품기능

TrustNET CA/RA 서버에서 인증서 발급을 위해 필요한 작업을 수행할 수 있도록 API 기능 제공

LRAPI

- ✓ TrustNET CA/RA 서버와의 암호화(https) 통신
- ✓ TrustNET CA/RA 서버에 사용자 등록/재등록, 삭제 요청
- ✓ TrustNET CA/RA 서버에 인증서 폐지 요청
- ✓ JAVA 1.3 이상의 모든 환경에서 사용 가능

Web Gateway

- ✓ TrustNET CA/RA 서버와의 암호화(https) 통신
- ✓ TrustNET CA/RA 서버 응답에 대해 TrustNET CA Client 에 무결성 검증 요청
- ✓ 사용자 등록 결과값인 참조번호, 인가코드를 이용하여 인증서를 발급 및 재발급
- ✓ 클라이언트에는 CA Client 가 설치되어 동작되어야 함
- ✓ JAVA 1.3 이상의 모든 환경에서 사용 가능

5. TrustNET CA Client

가. 제품 설명

나. 제품 기능

가.제품설명

PC Client

ActiveX Client

- ✓ ActiveX 로 제작 및 배포
- ✓ Windows Internet Explore 에서만 사용가능
- ✓ 사설 인증서를 발급받아 PC내의 File 형태로 저장
- ✓ 발급받은 사설인증서의 관리 기능 지원

TrustNET CA PC Client

발급된 인증서는 로컬 디렉토리에 File 형태로 보관되며,
Web Browser 또는 OS 종류에 따라
ActiveX / Non Plug-in 방식 2가지로 나뉩니다.

ActiveX Non Plug-in 2 Ways

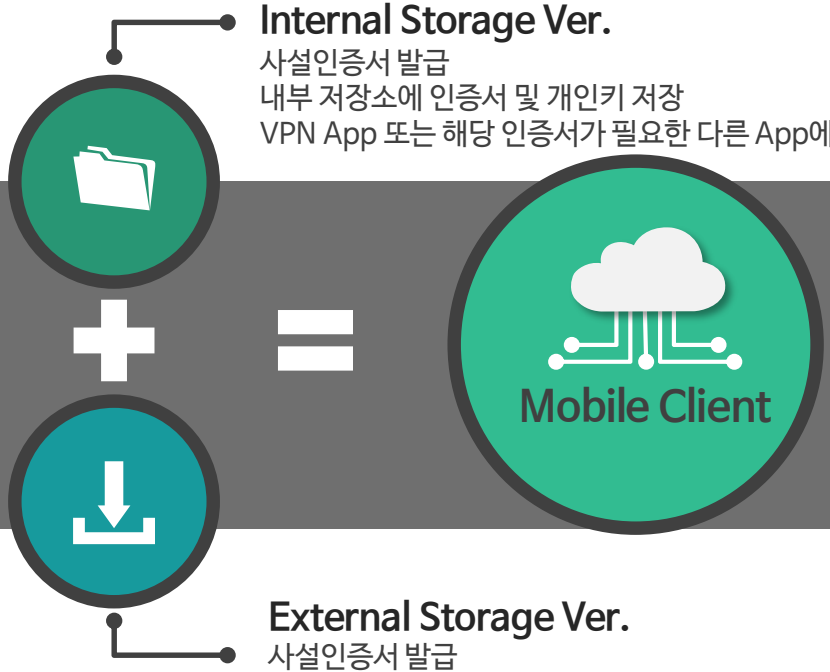
Windows - Internet Explore 환경에서는 ActiveX 모듈이 설치가 되며, 그 외 브라우저(chrome, safari, opera, firefox, Edge) 또는 OS 에서는 Non Plug-in 모듈이 설치되어 동작합니다.
각 모듈이 지원하는 기능은 동일합니다.

Non Plug-in Client

- ✓ Non Plug-in 방식의 모듈 제작 및 배포
- ✓ Internet Explore 환경을 포함한 브라우저 와 Windows 와 타 OS (Linux, MacOS) 환경에서 사용
- ✓ 사설 인증서를 발급받아 PC내 File 형태로 저장
- ✓ 발급받은 사설인증서의 관리 기능 지원

가.제품설명

Mobile Client



Internal Storage Ver.

사설인증서 발급
내부 저장소에 인증서 및 개인키 저장
VPN App 또는 해당 인증서가 필요한 다른 App에서 인증서 사용 가능

External Storage Ver.

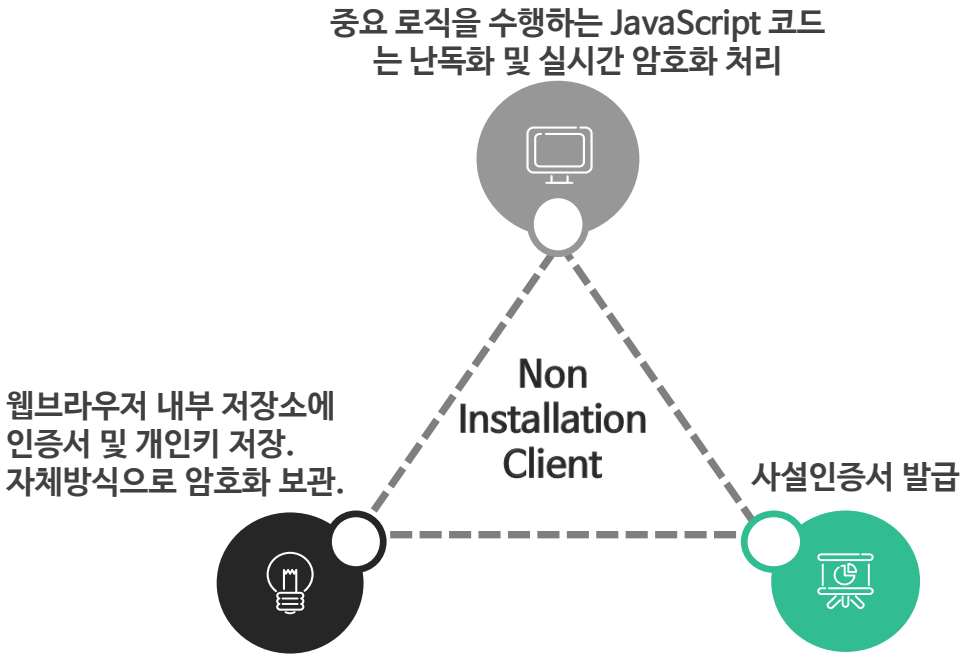
사설인증서 발급
외부 저장소에 인증서 및 개인키 저장
개인키 패스워드 변경
키/인증서 삭제

TrustNET CA Mobile Client는 스마트 폰 모바일 앱에 사설인증서를 발급 및 관리를 할 수 있는 기능을 제공합니다. 발급된 인증서의 저장형태에 따라 Internal Storage / External Storage 2가지 버전으로 나뉘며, Internal Storage는 클라이언트에서 인증서 발급 후 OS가 인식할 수 있는 내부 저장소에 저장 후 다른 App 또는 OS에서 인증서를 사용할 수 있고, External Storage는 SD Card 또는 App 내부 자체 폴더를 생성하여 저장하여, 인증서를 사용할 수 있는 기능을 제공합니다.

가.제품설명

Non Installation Client

JavaScript 와 HTML5 기술을 기반으로 Native 코드 없이 클라이언트 기능을 수행



- TrustNET Non-Native CA-Client는 JavaScript와 HTML5 기술을 이용하여 별도의 모듈을 설치할 필요 없이 PC, 모바일 환경에서 동일하게 사용할 수 있는 클라이언트 입니다.
- 발급된 인증서는 웹브라우저 내에 저장되어 사용되며, 안전하게 암호화되어 저장되므로 노출되거나 오용되거나 할 우려가 없습니다.

나.제품기능

제품 기능

TrustNET CA/RA 서버에 인증서 발급을 위해 필요한 작업을 수행할 수 있도록 API 기능 제공

PC Client

- ✓ TrustNET CA/RA 서버와의 데이트 무결성 검증 기능
- ✓ 인증서 발급에 필요한 인증서생성요청 정보 생성 및 인증서/개인키 저장 기능
- ✓ 인증서/개인키 삭제 기능, 개인키 비밀번호 변경 기능

Mobile Client

- ✓ TrustNET CA/RA 서버와의 데이트 무결성 검증 기능
- ✓ 인증서 발급에 필요한 인증서생성요청 생성 및 인증서/개인키 저장 기능
- ✓ VPN App 또는 다른 App 에서 인증서를 사용할 수 있도록 내부 저장소에 인증서세트를 저장하는 기능
- ✓ 외부 저장소에 인증서 저장 시 인증서/개인키 삭제 기능, 개인키 비밀번호 변경 기능

Non-Native Client

- ✓ TrustNET CA/RA 서버와의 데이트 무결성 검증 기능
- ✓ 인증서 발급에 필요한 인증서생성요청 생성 및 인증서/개인키 저장 기능
- ✓ 인증서/개인키 삭제 기능, 개인키 비밀번호 변경 기능
- ✓ 인증서 내보내기/들여오기 기능 제공

6. TrustNET Toolkit

가. 제품 설명
나. 제품 구성
다. 주요 기능
라. 특징 및 장점

가.제품설명

제품설명

TrustNET Toolkit

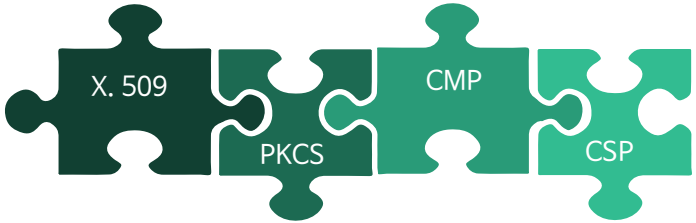
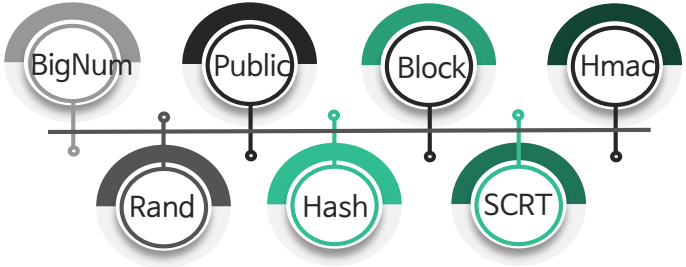
암호화 처리 API		전자서명 처리 API
응용관련기술	암호화관련기술	PKI관련기술 (IETF)

- 송수신 자료 암호화 기능(인증서 불필요)
- 송수신 자료 전자서명 기능(인증서 필요)
- 송수신 자료 무결성 제공(인증서 필요)
- 응용환경 사용자 인증 기능(인증서 필요)

나.제품구성

제품구성

SECURE APPLICATION

Toolkit(API)		각종 암호화 알고리즘 제공 (암호,전자서명, 해쉬, 랜덤넘버생성등..)
Cert Library		인증서(X509) 검증,경로검색 기능 암호문구 처리 기능 인증서 요청/폐지등 CA인터페이 기능 암복호자료 인코딩/디코딩
Crypto Library		서버 응용프로그램에서 암복호화 및 전자서명/검증 등에 대한 기능제공 레지스터리 및 스마트카드 인터페이스 지원

다.주요기능

주요기능(1/2)

구분	기능설명	특징
암복호화 기능	대칭키 알고리즘 및 공개키 알고리즘을 사용하여 특정 자료를 암호화/복호화 할 수 있는 기능	▪ 특정 자료 및 임의의 자료에 대한 암/복호화 가능 ▪ 첨부화일에 대한 암복호화 기능
전자서명 기능	특정 자료에 대해 전자 서명값을 생성하고 서명값을 검증하는 기능	▪ 첨부화일에 대한 전자서명 기능
암호화 키 생성 및 키 교환 기능	암복호화에 사용되는 세션 키(암호화키)를 안전하게 생성하여 교환(공유)할 수 있는 기능 제공	▪ SSL V3와 TLS V1.1에서의 키 공유 기능과 동일 방식
인증서 I/O 기능	인증서 및 개인 키를 레지스터리, 하드디스크, 스마트카드, USB포트등에 백업 및 복구할 수 있는 기능	▪ 다양한 형식의 저장형식 제공 (PKCS#12, PEM,DER 인코딩, 디코딩 기능) ▪ PKCS#8형태의 비밀키 관리
PKCS#7 메시지 (전자봉투) 기능	RSA의 표준 형식의 암복호화 및 전자서명 메시지 생성/복구 기능 지원	▪ 보안 메일, XML등에 대한 확장성 제공
인증서 검증기능	각종 인증기관에서 발급한 인증서에 대한 유효성 검증(경로검증) 기능 제공	

다.주요기능

주요기능(2/2)

구분	기능 설명	특징
공인인증기관 인증서 연동 기능	사내 사설인증서 및 공인인증기관 인증서를 통합하여 인터페이스 할 수 있는 기능 제공	▪ 6대 공인인증기관 발행 인증서 및 공인인증기관 상호연동 인증서 처리
인증서 관리 기능	인증서 발급요청 프로토콜인 CMP(Certificate Management Protocol) 방식에 의한 인증서 발급 신청 및 인증서 폐지, 인증서 갱신, 인증서 비밀번호 변경, 인증서 내보내기, 드려오기 등에 대한 기능 제공	▪ CMP 표준을 따르는 인증기관(공인인증기관 포함)은 모두 인터페이스 가능 ▪ 스마트 카드 및 USB 포트 등과의 인터페이스 제공
인증서 GUI(사용자 인터페이스) 기능	저장매체 별 인증서 선택 및 개인키 획득 등을 위한 편리한 화면 인터페이스 기능 제공	▪ 공인인증기관 인증서 처리 ▪ 인증서 자동선택 기능 제공
다양한 형태의 클라이언트 제공	ActiveX, Npruntime, 모바일, Non-Native 환경등 다양한 환경에 사용할 수 있는 클라이언트 제품을 제공 가능	▪ PC, 모바일 환경에서 사용되는 거의 모든 환경을 지원 가능 ▪ Non-Native 지원 클라이언트는 HTML5 기능을 지원하는 웹브라우저이어야 함.

라.특징및장점

특징 및 장점

맞춤형 툴킷제공

툴킷 구조가 3계층으로 구조화 되어 있으므로
고객이 원하는 기능만으로 가볍게 재구성 할 수 있음

관련 표준 완벽한 지원

국내 표준 알고리즘 지원, 기타 공개키 알고리즘 및
암호학적 표준의 완벽한 준수

공인 인증서 처리

현재 5개의 공인인증기관용 인증서 처리
(암복호화, 전자서명, 인터페이스, 스마트카드 지원)

속도 및 안정성 확보

멀티 쓰레드 환경을 고려한 설계에 따른 안전성 및
처리속도 보장(K전자서명/검증 시 약 0.03초)

다양한 환경 지원

웹To브라우저, 클라이언트To서버, 서버To서버 등
다양한 구조와 응용 환경 지원

다양한 구축 경험

제품사의 다양한 PKI 구축경험
(공인 및 대규모 인증센터구축, 다양한 공인인증기관 연동)


Thank you
UNET
유넷시스템