

보안을 보완하다

UCERT

SSL / CodeSign Certificate
Secure Email, VMC

기술지원

부서 | 기술지원팀

Tel 02-3442-7230

Mail dev_tech@ucert.co.kr

인증서 관련 문의

부서 | 인증사업팀

Tel 02-514-7786(대표)

Mail sales@ucert.co.kr

보안을 보완하다

UCERT

왜, 유서트일까요?

한국기업보안은 보안 시장과 함께 성장한
SSL 전문기업으로 오랜 경험을 통해
두터운 고객 신뢰 서비스를 구축하였습니다.

SSL 인증 분야의 전문인력들로 구성된
인증 사업부 유서트는 차별화된 서비스와
전문가만이 알 수 있는 오랜 기간 축적된 노하우로
고객 감동을 실현 하고 있습니다.

고객 만족을 넘어 고객 감동을 위한 서비스와
시장을 흔드는 혁신 마케팅으로
항상 비즈니스 파트너와의 가치를 최우선으로
성장하는 한국기업보안이 되겠습니다.

유서트에는 고객을 위한
특별한 서비스가 있습니다.

유서트 프리미엄 서비스

- ▶ 지정 담당 운영으로 신청에서 발급까지
One-Stop 서비스 제공
- ▶ 다양한 인증기관 보유
- ▶ 메일, SMS, 45일 전 전화까지 누락없는 갱신 관리
- ▶ 인증서 만료일 통합 서비스 제공
- ▶ 30일 무료 인증서 제공
- ▶ 체계화된 최고 기술 지원으로 장애 미처리율 0%



주요 강점

- KISA 보안서버전문협의회 소속
- 벤처기업인증
- 메인비즈 인증 획득
- AIG TECHPI 보험가입
- 1:1 지정 담당 서비스 제공
- 매년 매출 및 규모 상승
- SSL 기술연구소 운영
- 24,000건 기술지원 경력
- 장애 미처리율 0%
- 15년 보안서버 전문 판매
- 국내 최초 EV Codesign 판매
- 국내 최초 EV SSL 판매
- 무상 유지보수
- 365일 24시간 지원
- 국내 모든 서버 지원가능
- 무상 기술지원
- 네트워크 관련 특허 획득
- 인증서 컨설팅 지원

유서트 주요 고객사

유서트는 현재까지 200,000 여개의 인증서를 발급했습니다.



고객감동을 실천하는 기업, 한국기업보안 유서트입니다.

TLS/SSL Certificate

TLS/SSL은 인터넷 연결을 안전하게 유지하고 민감한 데이터를 보호하는 표준 기술입니다.

사용자와 웹사이트 간의 통신 또는 시스템 간의 전송되는 모든 데이터를 암호화하여, 전송 중인 데이터를 해독할 수 없도록 합니다.

SSL 인증서로 보호되는 웹사이트는 도메인의 주소가 https:// 로 표기되며, 인증서 정보는 브라우저의 주소 표시줄에서 자물쇠를 클릭하여 확인할 수 있습니다.



서비스 대상

- ▶ 개인정보 입력 구간이 있는 홈페이지를 운영하는 모든 공공기관 및 민간 기업 (회원가입, 로그인, 게시판 등)
- ▶ 데이터 전송 구간 암호화를 희망하는 모든 공공기관 및 민간 기업
- ▶ Server to Server, API 시스템의 https 암호화 통신이 필요한 모든 공공기관 및 민간 기업
- ▶ 안드로이드, IOS 앱 통신이 필요한 모든 공공기관 및 민간 기업
- ▶ 마이데이터(mTLS) 사업을 진행하고 있는 기업 (EV SSL 필수)

SSL 주요 기능

정보 유출 방지

Anti-sniffing

전송 구간 암호화
통신으로
안전한 데이터 전송

피싱 방지

Anti-phishing

CA의 도메인,
기업 인증을 받은
웹사이트만 발급 가능

Google 랭킹 상승

Google ranking rise

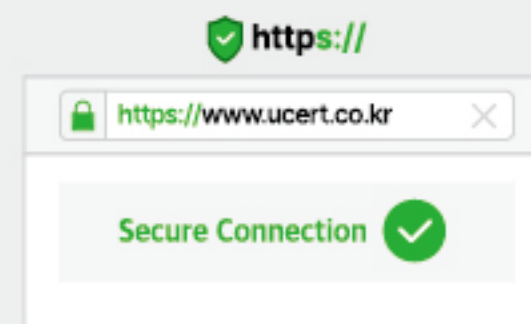
Google에서 https
보안연결 Site순위
결정 신호로 사용

RSA / ECC 암호화

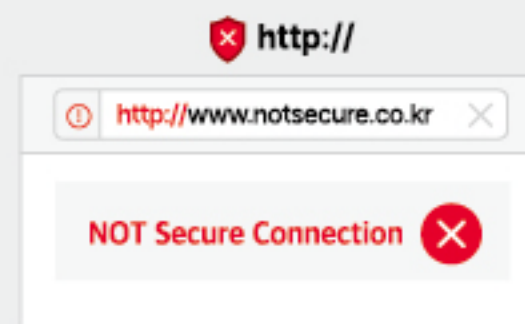
RSA/ECC encryption

RSA / ECC 암호화
알고리즘 지원

SSL 인증서가 적용되어 있는 웹사이트



SSL 인증서가 적용되어 있지 않은 웹사이트



인증기관 (Certificate Authority)

GlobalSign

digicert

SECTIGO

GOGETSSL

thawte

GeoTrust

Codesign Certificate

개발한 프로그램 및 어플리케이션을
CA(인증기관)의 인증서로 디지털 서명 후 온라인상으로 사용자들에게 배포 및 구동할 수 있도록 하는 인증서입니다.

디지털 서명된 프로그램은 명확한 게시자 확인으로
사용자가 안심하고 프로그램을 다운로드, 설치, 이용할 수 있도록 합니다.

2004년 전까지는 누구든지 배포할 수 있도록 되어있으나,
Microsoft사에서 2004년 8월에 출시한 Windows XP Service Pack2에서는
보안수준이 대폭 강화되어 인증이 되지 않은 응용프로그램의 경우
웹 브라우저에서 자동 차단되어 배포 자체가 불가능하게 되었습니다.



서비스 대상

- ▶ 보안프로그램, 드라이브 파일, EXE 파일 등 사용자가 웹사이트 사용에 필요한 프로그램을 배포하는 모든 공공기관 및 민간기업

CodeSign 주요 기능

	프로그램 무결성 입증 배포되는 프로그램의 최종서명 시점을 표시하여 무결성을 입증합니다.		악의적인 수정방지 서명된 파일은 수정 후 재서명이 필요하기 때문에 악의적인 수정이 불가능합니다.
	다양한 플랫폼 서명 Java, Apple, Visual Studio 등 다양한 플랫폼에서 서명을 진행할 수 있습니다.		EV인증서 드라이버 서명(.sys) 및 MicroSoft 인증이 필요한 경우에 사용됩니다.

프로그램이 정상적으로 서명되었을 때

Program_signing.exe 속성

일반	호환성	디지털 서명	보안	자세히	이전 버전
서명 목록					
서명자 이름 :		다이제스트 알고리즘	타임스탬프		
한국기업보안		sha256	2023년 1월 20일		
서명자 정보 확인 가능					

CodeSign 인증서 저장매체



- 스마트카드 기술이 적용된 휴대용 이중 인증 USB
- 보안 환경 내에서 개인 키, 비밀번호, 디지털 인증서와 같은 자격 증명을 생성·저장
- CC(공통 평가 기준) 인증, FIPS 인증 버전 이용 가능

Secure Email S/MIME

S/MIME 기술을 사용하여 사용자가 전자 메일에 디지털 서명하고 암호화 할 수 있도록 하는 인증서입니다.

전자메일에 디지털 서명을 사용하면,
전자메일의 내용이 전송 중에 변경되지 않았음을
보증하여 발신자를 증명할 수 있으며,

암호화된 이메일은 메시지 내용을 보호하고
중요정보가 타인의 손으로 넘어가지 않도록 방지합니다.



서비스 대상

- ▶ 개인정보, 금융정보 등의 중요 정보를 수/발신 하는 모든 민간 기업 및 공공기관
- ▶ FDA 승인을 위해 필요한 연구 보고서를 FDA에 발송하는 기업 및 기관
- ▶ 피싱메일 등의 이메일 해킹 위험을 줄이고 싶은 모든 민간 기업 및 공공기관

Secure Email(S/MIME)의 주요 기능



전자 메일 내용을
임의로 변경하는
위변조 방지



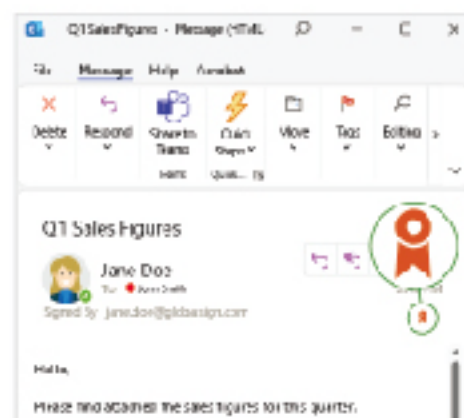
피싱, 스푸핑 된
메일과 구별하기 위한
이메일 발신자 확인



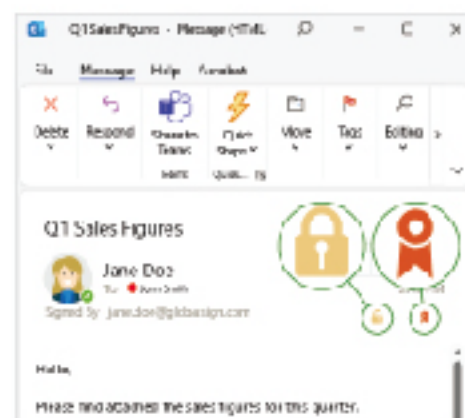
의도한 수신자만
암호화 된 메일에
액세스 가능

Secure Email(S/MIME)이 적용된 이메일

디지털 서명 된 이메일



서명 및 암호화 된 이메일



Secure Email(S/MIME)이 제공하는 보안 서비스

보안 서비스	보안 Mechanism	암호 알고리즘
메시지 기밀성	암호화	Triple-DES, RC2/40bit
메시지 무결성	해시함수	SHA-2, MD5
사용자 인증	공개키 인증	x.509 v3인증서
부인방지	전자 서명	DSS, RSA

VMC Certificate

회사가 고객의 받은 편지함에서
메시지를 열기 전에 “보낸 사람” 필드 옆에
상표가 등록된 로고를 표시 할 수 있는 인증서 입니다.

해당 로고는 도메인의 DMRAC상태와 조직의 인증된
신원을 시각적으로 확인해 주며,

VMC는 이메일 보안과 브랜드 보호를 강화하여
피싱 및 스푸핑 공격의 위험을 줄입니다.

받은 편지함



서비스 대상

- ▶ 사칭을 통한 피싱/스팸성 메일의 발송으로 인한 기업 신뢰성 및 브랜드 이미지의 저하를 우려하는 모든 기업 및 기관
 - ▶ 발신 기업의 로고가 보여져 다른 메일과 차별화된 브랜드 이미지를 원하는 모든 기업 및 기관
 - ▶ 엄격한 BIMi 정책을 거쳐 발신인의 무결성이 검증된 메일임을 보여주고 싶은 모든 기업 및 기관
- *BIMi = Brand Indicators for Message Identification

VMC(Verified Mark Certificate)의 주요 기능



BIMi 표준 준수를 통한 스팸성 메일의 수신 자체를 원천적으로 차단
(엄격한 수신지 스팸 판단 규정 및 수신 거부 정책)



수신 메일에서의 발신자의 브랜드 로고 표시를 통한
이미지 마케팅



로고가 없는 메일은 스팸으로 규정하여 간결하고
쾌적한 메일 서비스 운영

VMC 인증서가 적용된 이메일

