

PISFAIR2023

Track A Tech & Trend

Digital 시대의
WebTrust 와 Global CA

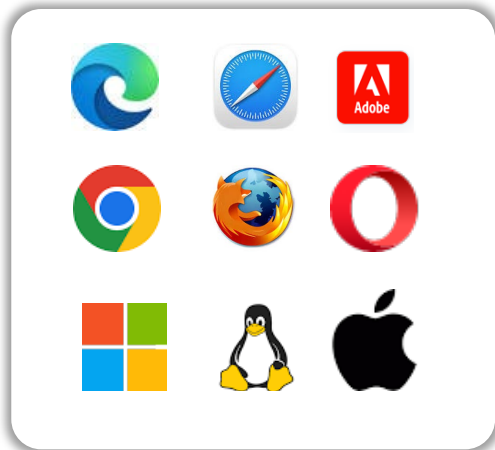
주식회사 한국기업보안



- 미국회계사협회(AICPA)와 캐나다회계사협회(CICA)가 참여하여 결성된 민간 컨소시엄
- Global CA (Certificate Authority) 인증에 필요한 점검 기준 개발
- Global CA (Certificate Authority) 인증 수행한 결과를 인정 해주는 기관
(운영 및 관리 능력의 신뢰성을 점검)
- 국내에서는 2021년 10월 국제통용평가 선정되어 고시 됨 (과학기술정보통신부)



OS & Browser



신뢰성 요청

기업들에 대한 검증

Global Certificate Authority



인증 기관에 대한 검증이 필요!

OS & Browser



객관적 검증 자료 제출 요구 // Root 저장

웹트러스트 감사 자료 제출

Global Certificate Authority



감사 요청



인정 승인

Enrolled
WebTrust
practitioners

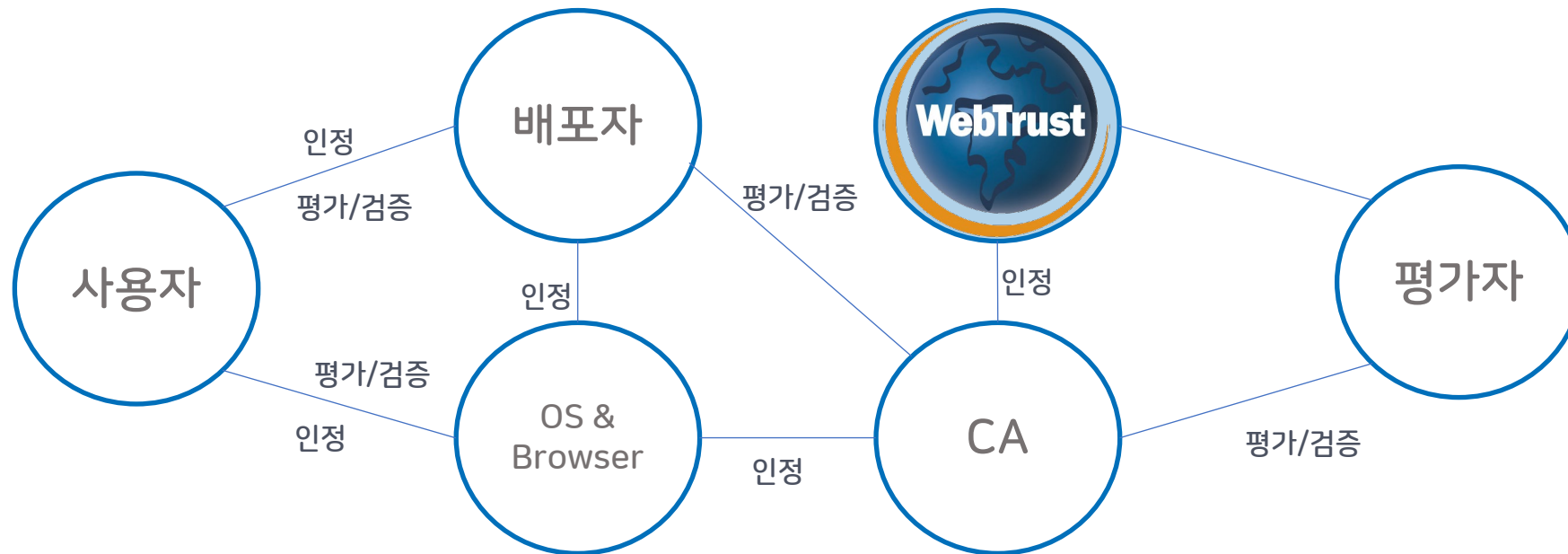
Deloitte, KPMG, EY

인증 기관에 대한 검증 수행

■ 웹트러스트 인증기관에 대한 원칙과 기준

- ① 인증기관 인증업무 공개
- ② 인증기관 인증업무 관리
- ③ 환경적 통제(시설 및 장비)
- ④ 인증기관 키 생명주기 관리
- ⑤ 가입자 키 생명주기 관리
- ⑥ 인증서 생명주기 관리
- ⑦ 하위인증기관 인증서 관리

약 420여개 평가 항목 감사

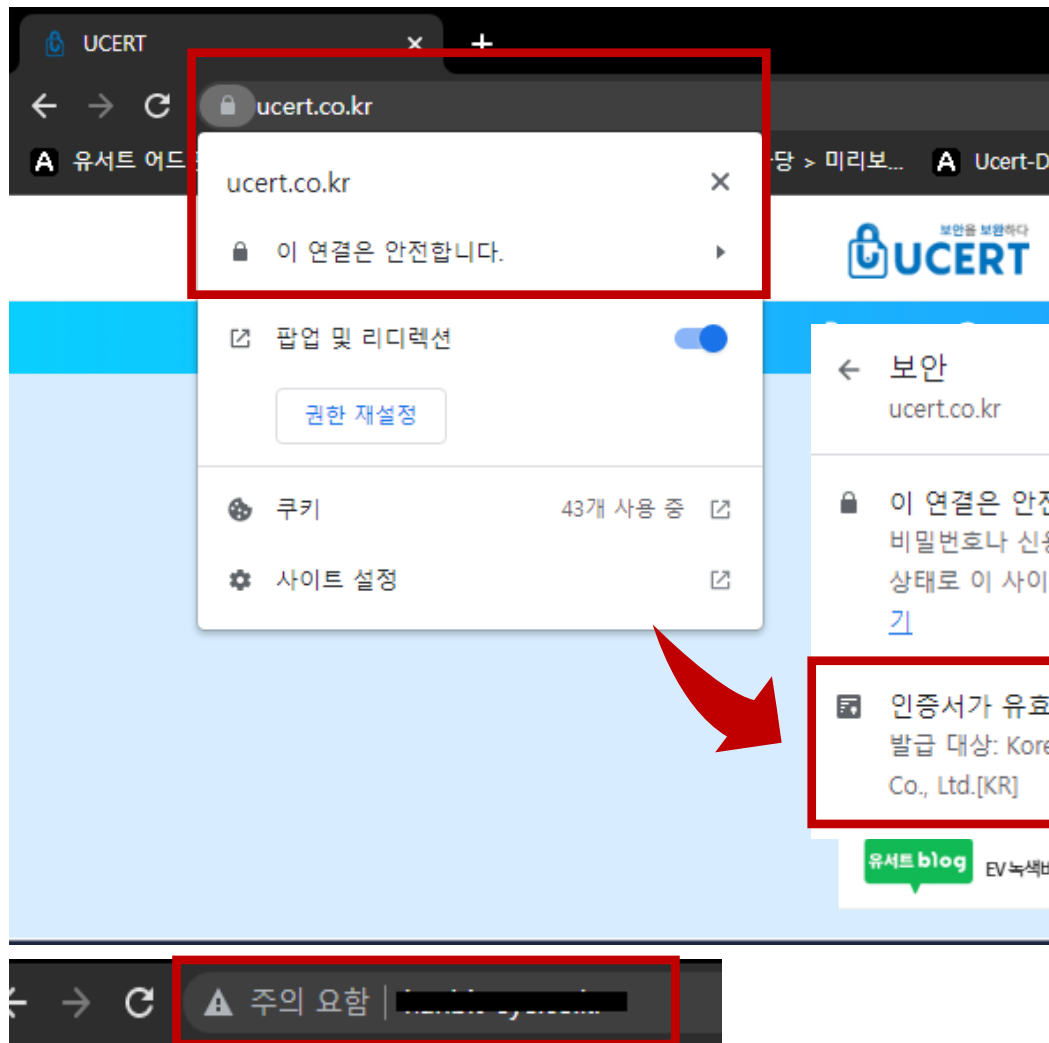


SSL / TLS Certificate

- End user 가 Browser를 통해 웹서버와 통신을 할 때 https (암호화 통신)을 지원
- WebTrust 인증을 받은 CA 가 웹서버를 운영하는 조직을 확인, 인증서 발급 (피싱 방지)
- 안전한 Web site 임을 확인 (신뢰성 확보)
- 국내에서는 개인정보보호법 기술적보호조치 대응 방안으로 보편화 됨
(개인정보보호법 시행령 제30조 개인정보의 안정성 확보 조치)



SSL / TLS Certificate



인증서 뷰어: www.ucert.co.kr

일반(G) 세부정보(D)

발급 대상

일반 이름(CN) www.ucert.co.kr
 조직(O) Korea Corporation Security Co., Ltd.
 조직 구성 단위(OU) <인증서에 속하지 않음>

발급 기관

일반 이름(CN) GlobalSign Extended Validation CA - SHA256 - G3
 조직(O) GlobalSign nv-sa
 조직 구성 단위(OU) <인증서에 속하지 않음>

유효성 기간

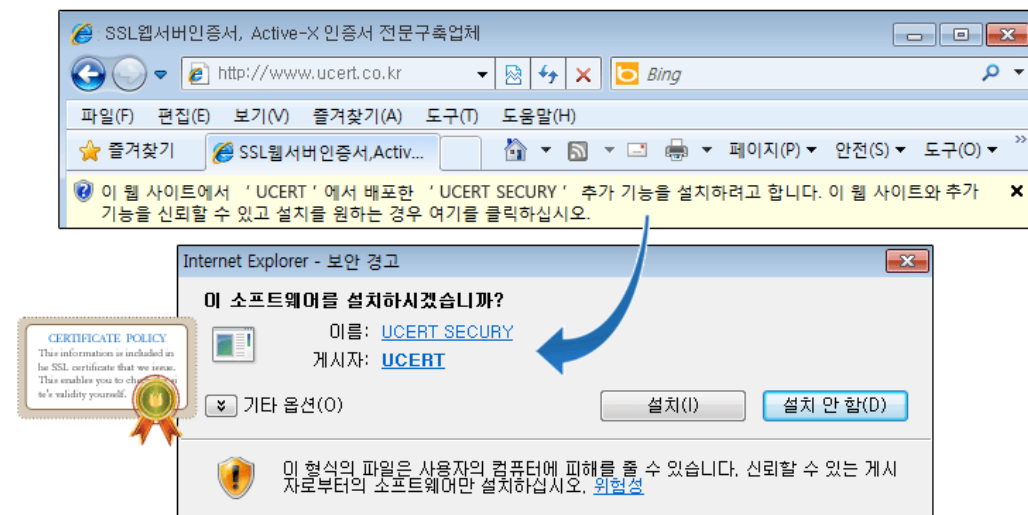
발급일: 2022년 8월 29일 월요일 오후 1:51:02
 만료일: 2023년 9월 30일 토요일 오후 1:51:01

지문

SHA-256 지문 B8 F7 2C 20 1E F0 78 D9 04 74 4E 19 43 FC 19 47
 D3 D5 9D 4F 76 1E AA 56 A2 BE 0C 4F 52 46 08 FC
 SHA-1 지문 05 77 0E 17 65 D5 68 22 1E 25 2B 4B F6 A4 9A EC
 E5 E1 4A 4C

Code Sign Certificate

- 배포하는 구동 프로그램의 배포자를 게시하여 사용자에게 무결성을 확인
- 배포 하려는 프로그램이 타인에 의해 수정되는 것을 방지



WebTrust - CA

디지털 서명(Digital Signature) - AATL Certificate

[디지털서명 필수 요건]

- 미국, EU , 주요 아시아 국가의 전자서명법, 디지털서명 관련 법적 효력 보유
- 무결성 유지 - 위조가 불가능 해야 함
- 서명자 인증 - 서명자의 개인 Key로 서명이 되어야 함
- 부인 방지 - 서명자가 서명 후에 서명 사실을 부인 하지 못하게 함
- 서명의 유효성 확인 - 서명 후 누구든 서명의 진위를 쉽게 확인 가능 해야 함

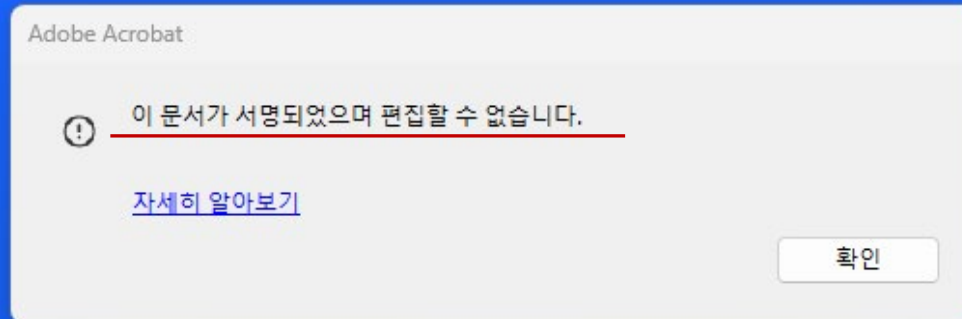


WebTrust - CA

디지털 서명(Digital Signature) - AATL Certificate



문서의 위조 변조 방지



TION

WebTrust - CA

디지털 서명(Digital Signature) - AATL Certificate

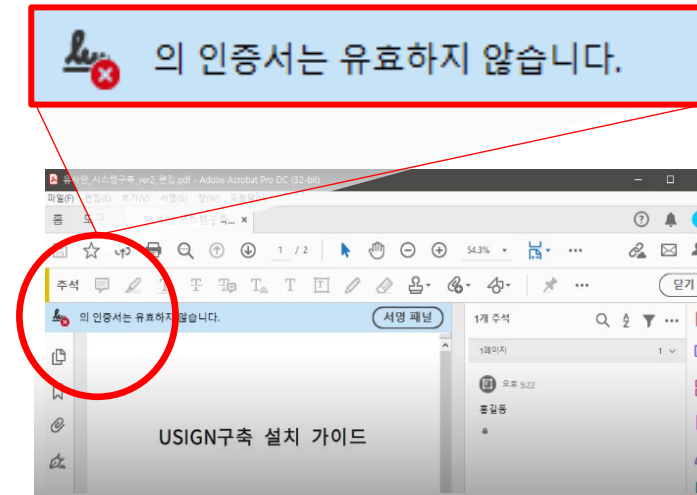


문서의 위조 변조 방지

[정상적인 문서의 표시]



[편집, 변조 되었을 때 나타나는 표시]



* File open access 디바이스의 상태가 오프라인 상태여도 유효성 검사는 가능함.

WebTrust - CA 디지털 서명(Digital Signature) - AATL Certificate



작성자, 서명자의 신원 확인

작성자 또는 서명자의 신원 확인이 문서 자체에서 즉시 확인 가능합니다.

공문서샘플4_sign.pdf - Adobe Acrobat Pro DC (32-bit)

파일(F) 편집(E) 보기(V) 전자 서명 창(W) 도움말(H)

홈 도구 공문서샘플4_sign.p... x

서명되었으므로 모든 서명이 유효합니다. 서명 패널

서명

모두 확인

수정 버전 1: Korea Corporation Security Co.,Ltd.

서명이 유효함:

신뢰할 수 있는 원본의 출처: Adobe Approved Trust

문서(는) 서명이 적용된 후 수정되지 않았습니

서명자의 ID가 유효합니다.

서명 시간은 서명자 컴퓨터의 시간을 기준으로 함

서명에 LTV를 사용하도록 설정되어 있음

서명 세부 사항

원인: 정윤미 (2021-12-30 18:08:01)

위치: 121.134.236.46

인증서 세부 사항...

필드: Signature11페이지

이 버전을 보려면 클릭하십시오.

주식회사 한국기업보안

주요 정보: 서울특별시 강남구 테헤란로 53 한국기업보안 TEL 02-534-7786 FAX 02-6008-7335

문서번호: 2021-1105-1

시행일자: 2021. 11. 05

수신: 0000 000 대표님,

발신: 주식회사 한국기업보안

목적: 000사와의 유사한 피호내 계약 전

1. 계약의 무공한 발원을 기원합니다.

2. 당사는 2021년 11월 05일 귀사와 유사한 계약을 체결하기로 하였습니다.

3. 당사는 계약기간 시작시점을 따라 2021.12.01일로 지정하고자 하오니, 검토를 부탁드립니다.

4. 다시 한번 귀사와 거래하여 주심에 감사드립니다.

주식회사 한국기업보안

주요 정보: 서울특별시 강남구 테헤란로 53 한국기업보안 TEL 02-534-7786 FAX 02-6008-7335

발행: 정윤미 본부장 02-534-7662

작성자, 서명자의 정보는 기업내 인사정보나 본인확인 기관의 (휴대폰인증, 공동인증서) 확인 정보를 기록 할 수 있습니다.

서명자의 조직명 확인

국제 공인 CA에서 검증한 조직명 기록

서명자의 신원

본인확인 수단으로 부터 전송 받은 데이터

서명 시각, 서명 위치 확인

국제 공인 TSA (타임스탬프) 사용

WebTrust - CA 디지털 서명(Digital Signature) - AATL Certificate



서명시간과 서명 장소의 기록과 보존

디지털 서명이 사용된 문서는 **작성시간, 서명 시간이 국제 표준 시간으로 기록 됩니다.**

공문서샘플4_sign.pdf - Adobe Acrobat Pro DC (32-bit)

파일(F) 편집(E) 보기(V) 전자 서명 창(W) 도움말(H)

홈 도구 공문서샘플4_sign.p... x

서명되었으며 모든 서명이 유효합니다.

서명

모두 확인

수정 버전 1: Korea Corporation Security Co., Ltd.

서명이 유효함:

신뢰할 수 있는 원본의 출처: Adobe Approved Trust List (AATL).

문서(는) 서명이 적용된 후 수정되지 않았습니다.

서명자의 ID가 유효합니다.

서명 시간은 서명자 컴퓨터의 시간을 기준으로 합니다.

서명 시간(2021/12/30 18:08:01 +09'00')에 서명 유효성을 검사했습니다.

서명자 정보

서명자의 인증서에서 발급자의 인증서까지의 경로가 작성되었습니다.

서명자의 인증서가 유효하며 해지되지 않았습니다.

서명자 인증서 표시(S)...

고급 속성(A)... 서명 유효성 검사(V) 닫기(C)

원인: 정윤미 (2021-12-30 18:08:01)
위치: 121.134.236.46

유효성 요약

서명이 적용된 후 문서이(가) 수정되지 않았습니다.

인증자가 이 문서에 대해 양식 채우기, 서명 및 주석 달기를 허용했습니다. 다른 사항은 변경할 수 없습니다.

서명자의 ID가 유효합니다.

서명 시간은 서명자 컴퓨터의 시간을 기준으로 합니다.

서명 시간(2021/12/30 18:08:01 +09'00')에 서명 유효성을 검사했습니다.

서명자 정보

서명자의 인증서에서 발급자의 인증서까지의 경로가 작성되었습니다.

서명자의 인증서가 유효하며 해지되지 않았습니다.

서명자 인증서 표시(S)...

고급 속성(A)... 서명 유효성 검사(V) 닫기(C)

원인: 정윤미 (2021-12-30 18:08:01)
위치: 121.134.236.46

인증서 세부 사항...

마지막으로 확인한 날짜: 2021.12.30 18:08:01

필드: Signature11페이지

이 버전을 보려면 클릭하십시오.

우편 08027 서울특별시 서초구 강남대로 99길 53 원우빌딩 4층 한국기밀보안 TEL 02-534-7788 FAX 02-6098-7335
담당 : 정윤미 본부장 02-534-7662

서명시간 및 서명 위치 확인

원인: 정윤미 (2021-12-30 18:08:01)
위치: 121.134.236.46

작성자, 서명자의 Device의 시간을 변경해도
국제 공인 타임스탬프 시간이 기록 되어, 시간 변조, 위치 변조가
불가능 합니다.

WebTrust - CA

디지털 서명(Digital Signature) - AATL Certificate

E-signature Grade

Grade criteria of e-signatures

QES (Qualified e-Signatures)

AES 와 SES를 포함하는 고급 디지털 서명 방식을 말합니다.

제 3자가 검증한 조직의 디지털 인증서로 서명 되어야 한다.

각 국가 또는 조직이 인정하는 개인의 식별 정보가 포함 되어야 한다.

위조 변조 방지 기능을 포함 해야 한다.

Digital Signature

AES (Advance e-Signatures)

서명자와 서명 요청자의 서명 연결이 유지 되어야 하고, 서명자 식별이 가능 해야 한다.

서명자의 서명에 서명 대표성이 있어야 한다.

서명 후 위조, 변조 식별 기능을 보유 해야 한다.

SES (Simple e-signatures)

서명자의 특별한 추가적인 신원 확인 없이 지정된 서명예정자의 이메일 등으로 전송 하여 이미지 업로드 서명을 하는 기준



Never trust, Always verify

15년 기업 전문 기업, 한국기업보안이 기업 솔루션의 기준을 바꿉니다.

레퍼런스

SSL 보안서버
누적 건수
122,174건

기업 고객사
약 9,700개 보유
(연간)

Partner
154개

Our Business



점유율 1위 사업자



국제통용, 국내 특허 획득



웹취약점 점검
개인정보 현장 점검 사업



캐릭터 사업

2021' 과학기술정보통신부 장관상 수상

2020' SSL 보안서버 구축 점유율 1위

강소기업 | 벤처인증 | GS인증 | 메인비즈인증

감사합니다

보안을 보완하다



한국기업보안

Korea Corporation Security

usign.kr | ucert.co.kr

usign

최제
jchoe@korsec.co.kr
010-6232-9283

송신영 과장
ssy@korsec.co.kr
010-4878-5364

UCERT

황이혜 팀장
hih@korsec.co.kr
02-514-7786

박찬호
pch@korsec.co.kr
02-514-7786