Sectigo
eToken(USB) 서명 가이드

[고객센터]
한국기업보안. 유서트 기술팀
02-3442-7230

한국기업보안
Korea Corporation Security

목 차

※ 토큰 패스워드 주의사항

Safenet eToken 5110cc의 토큰은 인증을 위해 다양한 비밀번호를 사용합니다.
관리자 암호 5회, PUK/PIN 3회 잘못 입력하면 eToken이 영구적으로 잠기게 되며 사용할 수 없습니다.
관리자 암호, PUK/PIN 암호 분실 및 잠김으로 인해 토큰 사용을 못하게 되는 경우, 새로운 토큰을 구매해야 함을 안내 드립니다.

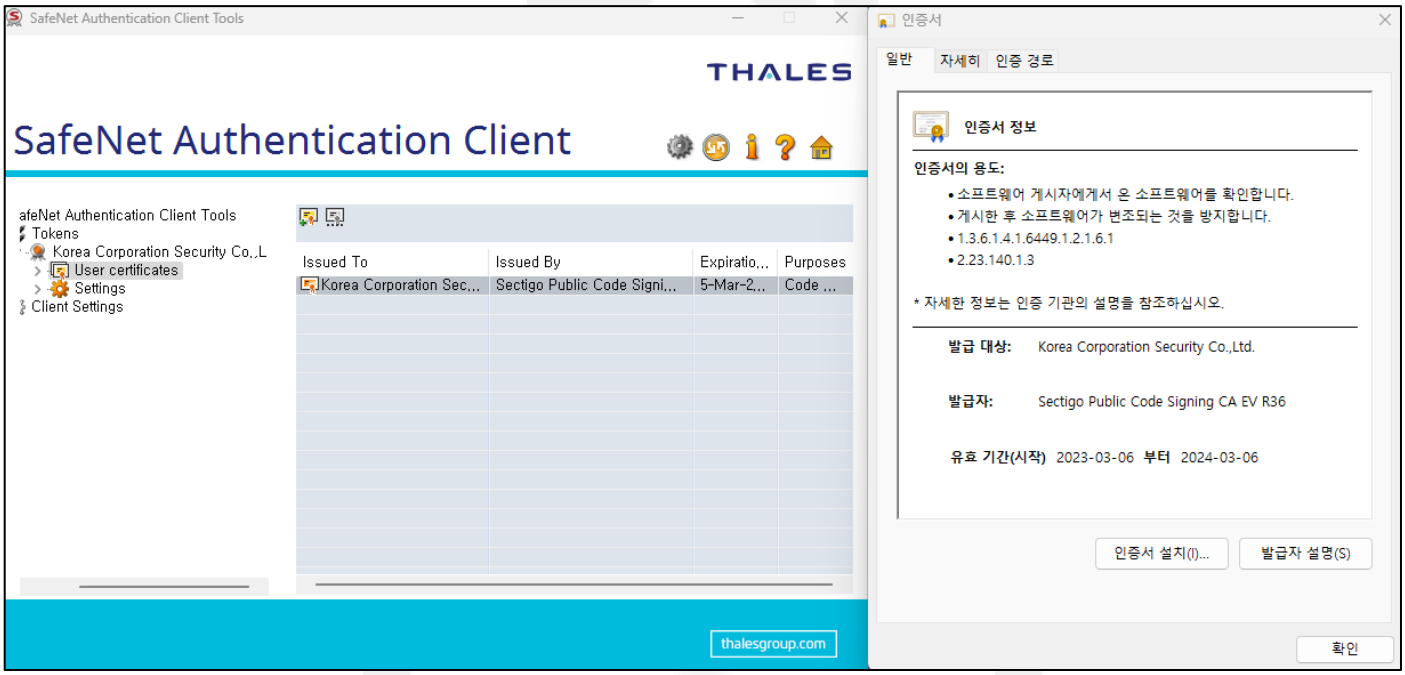
***참고**

1. 토큰 암호 : eToken 인증서 저장소에 액세스하는데 사용됩니다. (패스워드 분실 시, 재설정 가능)
2. 관리자 암호 : eToken을 관리 하기 위해 사용합니다. (패스워드 분실 시, 토큰 사용 불가)
3. PUK(Personal Unlocking Key) : 기본 PUK 패스워드 000000 (패스워드 분실 시, 토큰 사용 불가)

Step1. 인증서 정상 등록 여부 확인

Safenet 프로그램을 클릭하여 Safenet Token(USB)에 아래와 같이 인증서가 추가되어있는지 확인합니다.

사용자 인증서 > 발급 대상의 인증서 더블클릭하여 인증서 만료일자 확인



Step2. 디지털 서명하기

1. 서명에 필요한 SDK 설치
(이미 SDK 를 보유하고 있는 경우, 해당 SDK는 설치하실 필요가 없습니다.)

SDK 파일 다운로드 : https://developer.microsoft.com/en-us/windows/downloads/sdk-archive

설치 된 SDK 폴더 위치인 "C:₩Program Files (x86)₩Windows Kits₩10₩App Certification Kit" 경로 이동.
(설치 위치와 버전에 따라 설치 경로가 달라질 수 있습니다.)
"signtool.exe"파일이 존재하는 위치에 서명할 파일을 동일하게 위치시킵니다.
("sample.exe" 파일은 예시로 생성한 파일입니다.)

2. 서명 하기

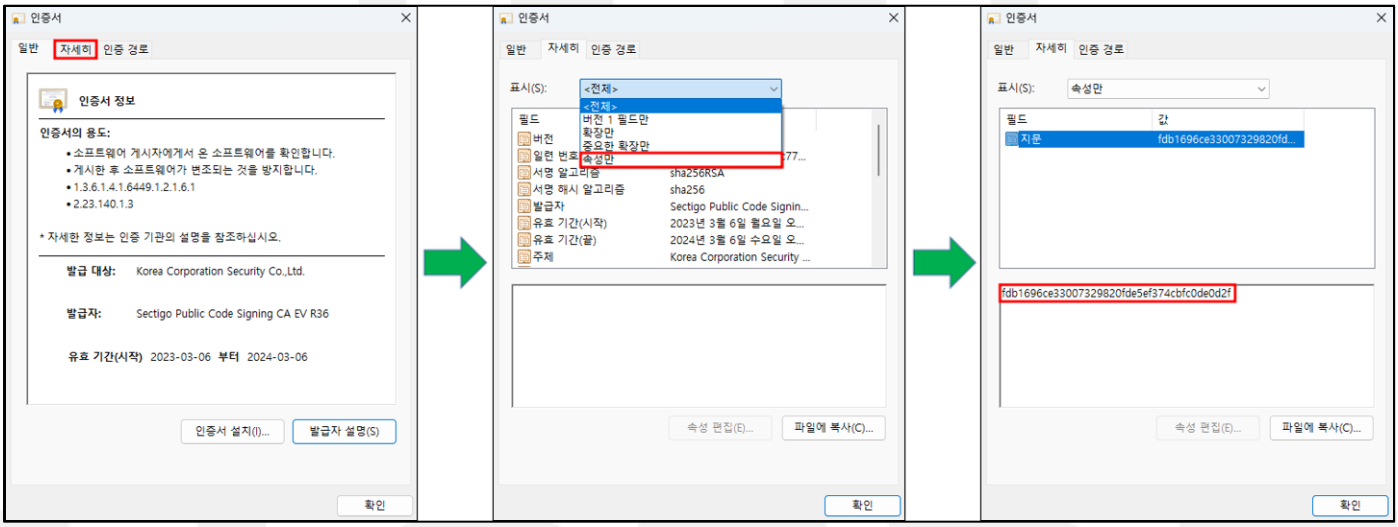
1) 다이제스트 알고리즘 SHA2 서명 하기

1-1) 명령 프롬프트창(cmd : 관리자권한으로 실행 권장)에서 signtool 이 있는 경로로 이동

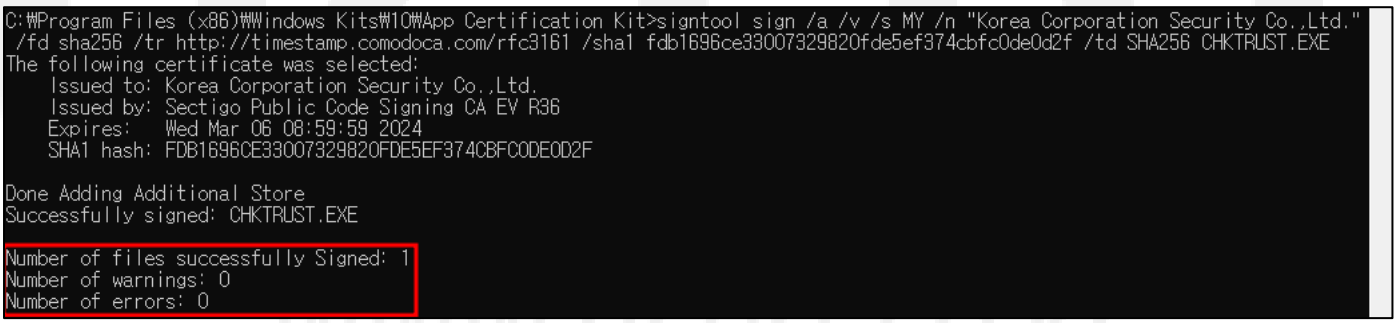
1-2) 서명 명령어 입력

signtool sign /a /v /s MY /n [게시자명] /as /fd sha256 /tr http://timestamp.comodoca.com/rfc3161 /sha1 *[지문값] /td SHA256 [서명할 파일]

* 지문값 확인하는 방법



1-3) 서명 명령어 입력 후 메시지 확인



1-4) 명령 프롬포트창에서 인증서 확인하기

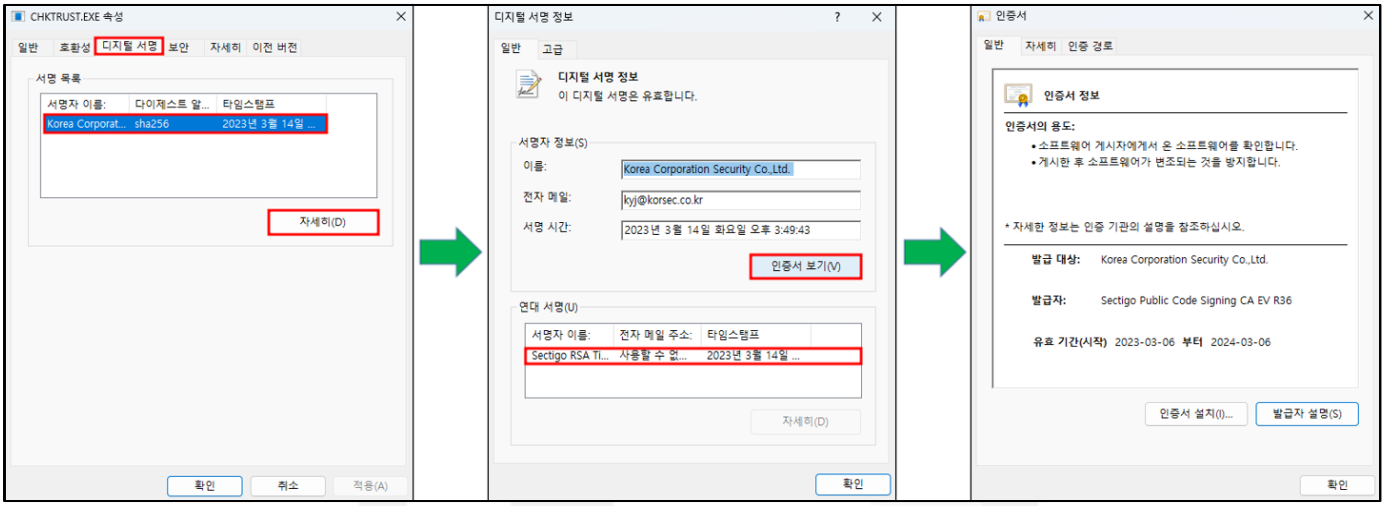
signtool.exe verify /v /pa [서명한 파일명]

아래 표시된 Signing Certificate Chain 부분 처럼 4개의 인증서로 보여진다면 정상 서명된 것을 의미합니다.

```
C:₩Program Files (x86)₩Windows Kits₩10₩App Certification Kit>signtool.exe verify /v /pa CHKTRUST.EXE

Verifying: CHKTRUST.EXE

Signature Index: 0 (Primary Signature)
Hash of file (sha256): 4EAEA6D794D98E27E3DAEDC6A77296274A1B3339E150110DFD3D50FD7E2A368C

Signing Certificate Chain:
    Issued to: AAA Certificate Services
    Issued by: AAA Certificate Services
    Expires:   Mon Jan 01 08:59:59 2029
    SHA1 hash: D1EB23A46D17D68FD92564C2F1F1601764D8E349

        Issued to: Sectigo Public Code Signing Root R46
        Issued by: AAA Certificate Services
        Expires:   Mon Jan 01 08:59:59 2029
        SHA1 hash: 329B78A5C9EBC2043242DE90CE1B7C6B1BA6C692

            Issued to: Sectigo Public Code Signing CA EV R36
            Issued by: Sectigo Public Code Signing Root R46
            Expires:   Sat Mar 22 08:59:59 2036
            SHA1 hash: 0185FF9961FF0AA2E431817948C28E83D3F3EC70

                Issued to: Korea Corporation Security Co.,Ltd.
                Issued by: Sectigo Public Code Signing CA EV R36
                Expires:   Wed Mar 06 08:59:59 2024
                SHA1 hash: FDB1696CE33007329820FDE5EF374CBFC0DE0D2F

The signature is timestamped: Tue Mar 14 15:49:43 2023
Timestamp Verified by:
    Issued to: AAA Certificate Services
    Issued by: AAA Certificate Services
    Expires:   Mon Jan 01 08:59:59 2029
    SHA1 hash: D1EB23A46D17D68FD92564C2F1F1601764D8E349

        Issued to: USERTrust RSA Certification Authority
        Issued by: AAA Certificate Services
        Expires:   Mon Jan 01 08:59:59 2029
        SHA1 hash: D89E3BD43D5D909B47A18977AA9D5CE36CEE184C

            Issued to: Sectigo RSA Time Stamping CA
            Issued by: USERTrust RSA Certification Authority
            Expires:   Tue Jan 19 08:59:59 2038
            SHA1 hash: 02D65B95E28370C1570095FA88F923DD937FAD8F

                Issued to: Sectigo RSA Time Stamping Signer #3
                Issued by: Sectigo RSA Time Stamping CA
                Expires:   Thu Aug 11 08:59:59 2033
                SHA1 hash: AB34013AAC4097319F081AF0B318E183F80F7881


Successfully verified: CHKTRUST.EXE

Number of files successfully Verified: 1
Number of warnings: 0
Number of errors: 0
```

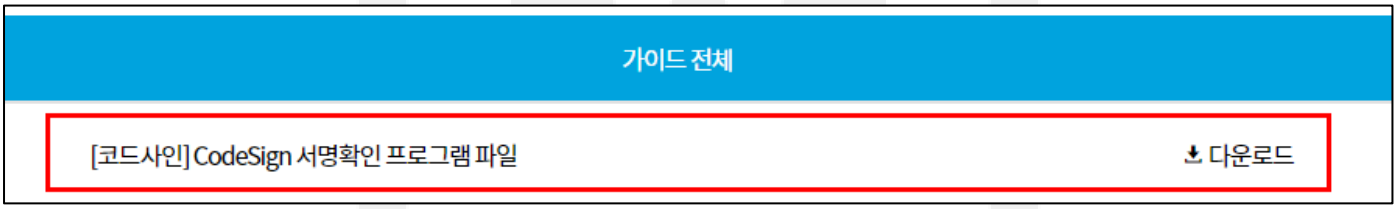
1-5) 서명 확인 하기

서명된 exe 파일의 속성에서 디지털 서명 내역 확인



1-6) 게시자 확인 하기

CHKTRUST.EXE 프로그램 다운로드 : https://www.ucert.co.kr/board/list/guide/codesign

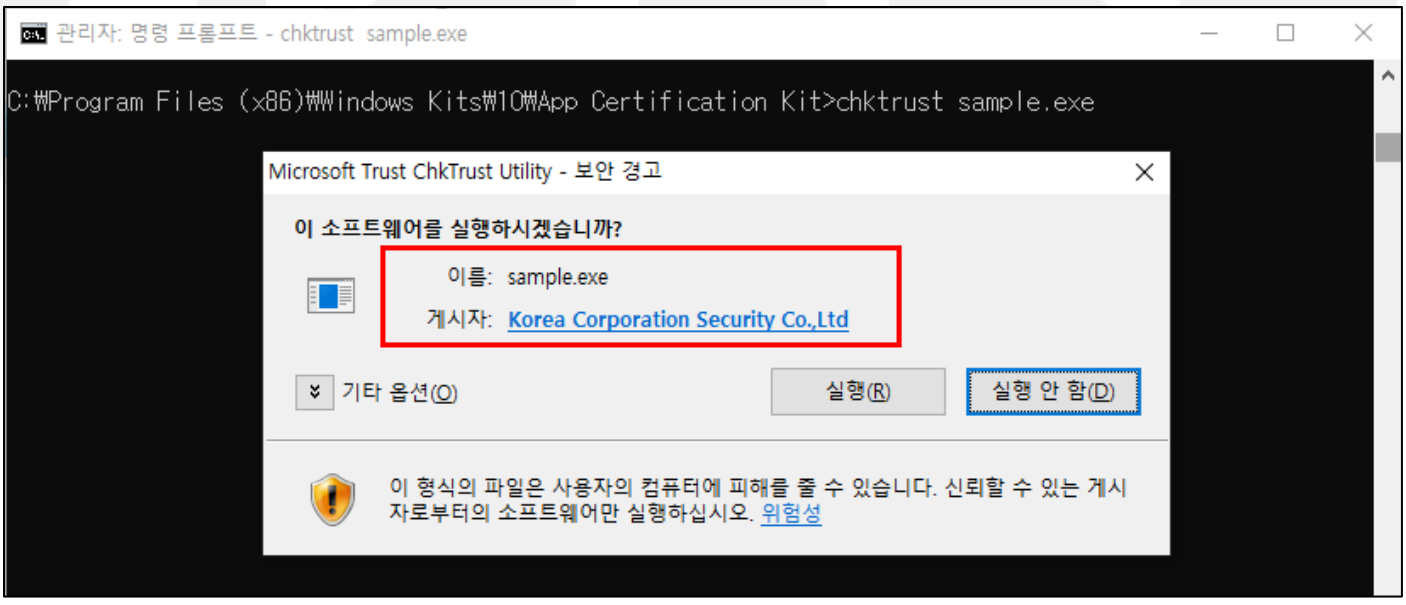


*** CHKTRUST.EXE 프로그램의 위치와 서명된 파일이 동일한 위치에 있지 않을 경우, 경로를 지정해주셔야 합니다.**

게시자 확인 명령어 :

```
chktrust [파일명]
```

예시)



2) 드라이버 서명 하기(.sys 파일 서명) – EV CodeSign 사용자만 가능

2-1) 드라이버 서명 방법은 상단 서명 하기와 동일하며, 서명 후 Microsoft 하드웨어 프로그램 등록이 필요합니다.

2-2) 서명된 파일을 Microsoft 하드웨어 프로그램 등록 진행
드라이버 프로그램을 배포할 경우, 마이크로소프트 드라이버 서명 배포 프로세스 절차에 따라 마이크로 소프트에 서명된 파일을 제출해야 합니다.

https://docs.microsoft.com/en-us/windows-hardware/drivers/dashboard/register-for-the-hardware-program
업체 등록 후, EV 코드사인으로 서명한 파일을 제출(비용 무료/ 소요시간 약 1주일 소요)

※ 이전에 서명하여 배포된 프로그램은 영향 받지 않으며,
신규 서명시에 마이크로소프트 프로세스 절차를 확인하신 후, 진행해 주셔야 합니다.

3. CodeSign 주요 옵션 안내

Sign 명령 주요 옵션	설명
/a	가장 적합한 서명 인증서를 자동으로 선택합니다. 서명 도구는 지정한 모든 조건을 만족하는 유효한 모든 인증서를 찾아서 최대 시간 동안 유효한 인증서를 선택합니다. 이 옵션이 없으면 서명 도구는 유효한 서명 인증서를 하나만 찾게 됩니다.
/v	명령이 성공적으로 실행되는지 또는 실패하는지 여부와 상관없이 자세한 정보 출력을 표시하고 경고 메시지를 표시합니다.
/as	이 서명을 추가합니다. 주 서명이 없으면, 이 서명이 기본 서명을 대체합니다.
/s *StoreName*	인증서를 검색할 때 열 저장소를 지정합니다. 이 옵션을 지정하지 않으면 My 저장소가 열립니다.
/fd	파일 서명을 만드는 데 사용할 파일 다이제스트 알고리즘을 지정합니다. 참고: 서명 중에 /fd 스위치가 제공되지 않으면 경고가 생성됩니다. 기본 알고리즘은 SHA1 이지만 SHA256 을 권장합니다.
/tr *URL*	RFC 3161 타임스탬프 서버의 URL 을 지정합니다. 이 옵션(또는 /t)이 없으면 서명 파일에 타임스탬프가 기록되지 않습니다. 타임스탬프 기록에 실패하면 경고가 생성됩니다. 이 옵션은 /t 옵션과 함께 사용할 수 없습니다.
/td *alg*	/tr 옵션을 사용하여 RFC 3161 타임스탬프 서버에서 사용하는 다이제스트 알고리즘을 요청합니다. 참고: 타임스탬프 처리 중에 /td 스위치가 제공되지 않으면 경고가 생성됩니다. 기본 알고리즘은 SHA1 이지만 SHA256 을 권장합니다.
	/td 스위치는 /tr 스위치 앞이 아니라 뒤에서 선언되어야 합니다. /td 스위치가 /tr 스위치 앞에서 선언되면 의도된 SHA256 알고리즘이 아닌 SHA1 알고리즘에서 타임스탬프가 반환됩니다.
/fd *certHash*	문자열 *certHash* 를 지정하면 서명 인증서에 사용되는 알고리즘이 기본값으로 설정됩니다.
	참고: Windows 10 키트 빌드 20236 이상에서만 사용할 수 있습니다.
/n *SubjectName*	서명 인증서의 주체 이름을 지정합니다. 이 값은 주체의 전체 이름에서 부분 문자열이 될 수 있습니다.
/p *Password*	PFX 파일을 열 때 사용할 암호를 지정합니다. (/f 옵션을 사용하여 PFX 파일을 지정합니다.)
/u *Usage*	EKU(확장된 키 사용)가 서명 인증서에 있도록 지정합니다. 용도 값은 OID 또는 문자열로 지정될 수 있습니다. 기본 용도는 "코드 서명"(1.3.6.1.5.5.7.3.3)입니다.

참고 : https://docs.microsoft.com/ko-kr/dotnet/framework/tools/signtool-exe