Code Signing

인증서 설치 매뉴얼

매뉴얼 구성

1.관련 툴 참고 링크

2.MS

2.1 User Mode sign

2.2 Kernerl Mode sign

2.3 Dual sign

2.4 정상 서명 확인 방법

3. Java

4. code 관련 이슈 정리

1.관련 툴 참고 링크

MS (signtool.exe)

Microsoft SDK가 포함된 패키지의 다운로드링크입니다.

Windows 7

https://www.microsoft.com/en-us/download/details.aspx?id=8279

Windows 8.1

https://dev.windows.com/ko-kr/downloads/windows-8-1-sdk

windows 10

https://dev.windows.com/en-us/downloads/windows-10-sdk

Signtool.exe 옵션 설명 링크

http://msdn.microsoft.com/en-us/library/windows/desktop/jj835835(v=vs.85).aspx

java (jarsigner)

http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html

2.MS

준비사항

(관련폴더를 지정하여 관련 파일을 모두 이동시켜 놓으시면 작업이 편리합니다-권장-)

User Mode sign

한국전자인증에서 전달

cert.pfx

작업자가 준비할 것

signtool.exe

서명되어 배포될 파일

Dual sign

한국전자인증에서 전달

cert.pfx(sha1), cert.pfx(sha2)

(해당 파일명은 작업자가 구분을 위하여 변경하시면 작업이 편합니다.-권장-)

Ex) cert-sha1.pfx, cert-sha2.pfx

작업자가 준비할 것

signtool.exe

서명되어 배포될 파일

Kernerl Mode sign

한국전자인증에서 전달

cert.pfx, MSCV-VSClass3.cer

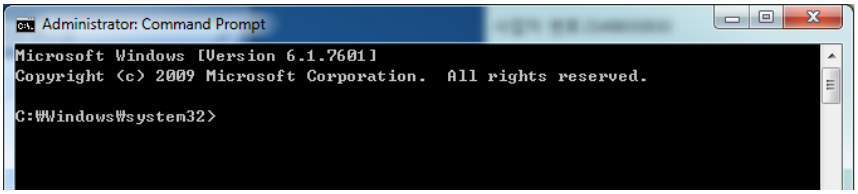
작업자가 준비할 것

signtool.exe

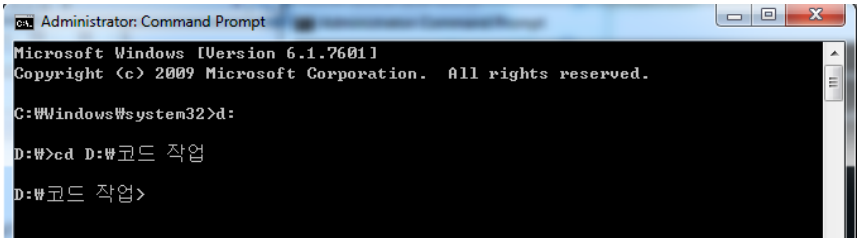
서명되어 배포될 파일

2.1 User Mode sign

명령프롬프트를 관리자의 권한으로 시작합니다.



관련 폴더로 이동합니다.



서명 명령어는 다음과 같습니다.

signtool.exe sign /f cert.pfx /p "비밀번호" /d "설명" /du "배포사이트url" /fd sha256 /t http://timestamp.verisign.com/scripts/timstamp.dll "test.cab"

(/fd sha256은 winsdows7이상에서만 사용하시기 바랍니다.(-권장-) xp에서는 /fd sha1으로 진행하셔야 합니다.)

서명을 위한 최소한의 명령어는 다음과 같습니다.

signtool sign /a /f cert.pfx /p 비밀번호 서명할파일명

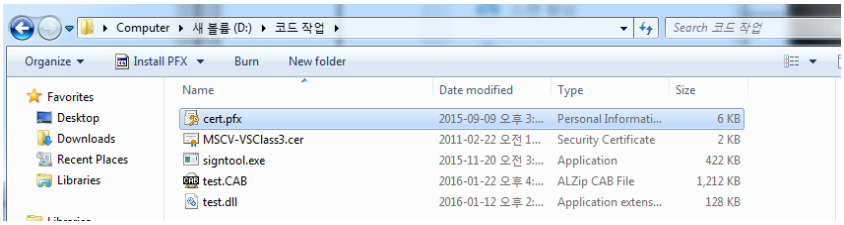
서명 명령어의 예시입니다.

signtool.exe sign /f cert.pfx /p 1234 /d Test /du http://www.test.com /fd sha1 /t http://timestamp.verisign.com/scripts/timstamp.dll test.cab

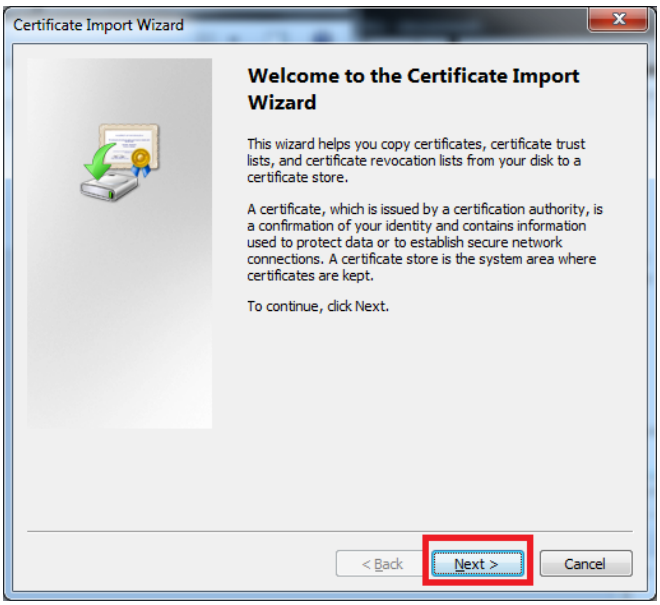
```
D:₩코드 작업>signtool.exe sign /f cert.pfx /p 1234  /d Test /du http://www.test.
com /fd sha1 /t http://timestamp.verisign.com/scripts/timstamp.dll test.cab
Done Adding Additional Store
Successfully signed: test.CAB
```

2.2 Kernerl Mode sign

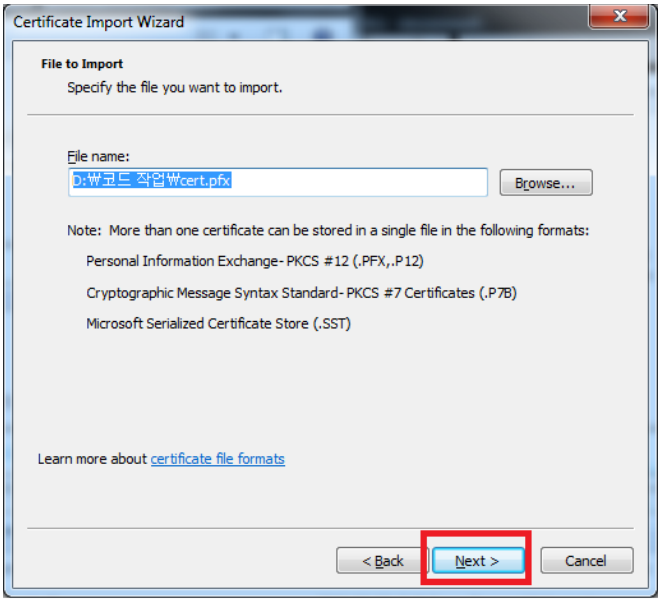
인증서 등록



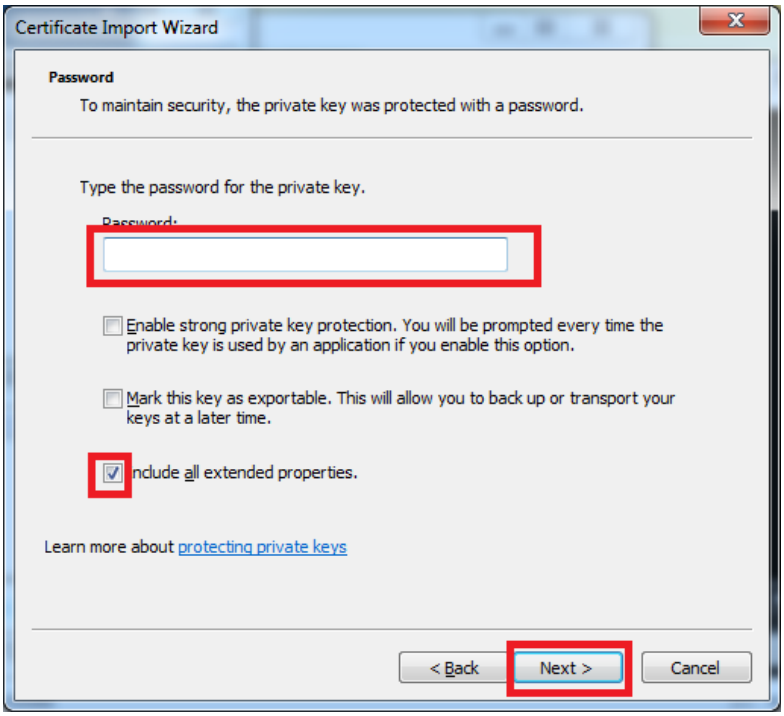
Cert.pfx를 실행합니다.



다음을 선택합니다

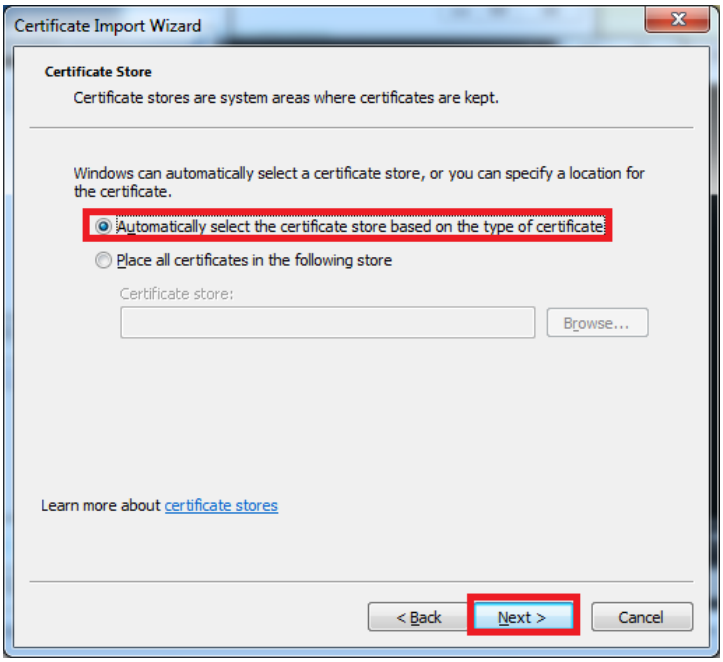


경로 확인하고 다음을 선택합니다

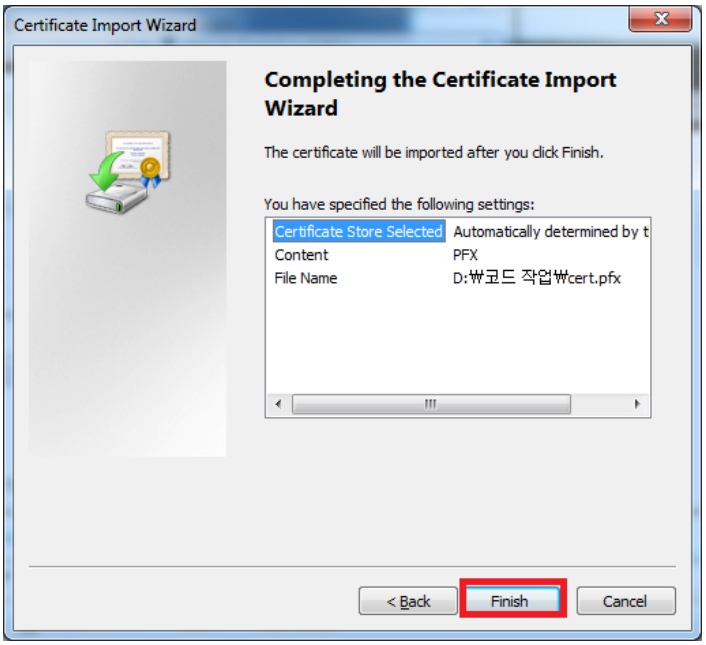


패스워드를 입력하고 다음을 선택합니다

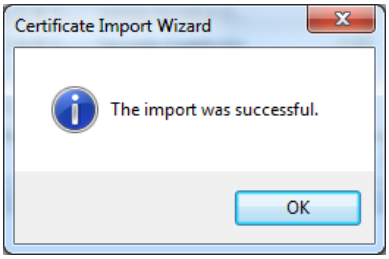
(3번째 박스에 클릭하여 지정된 체인을 함께 불러옵니다.)



자동으로 경로설정을 선택하고 다음을 선택합니다.

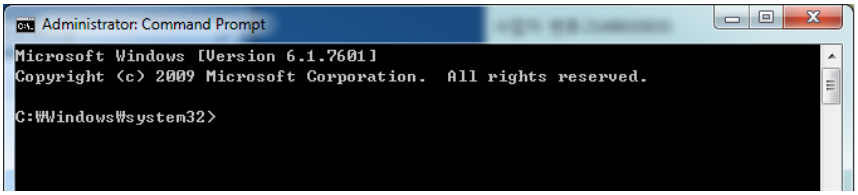


마침을 선택합니다.

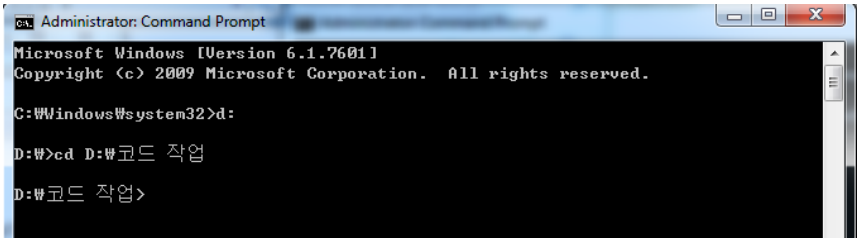


인증서 설치가 모두 완료되었습니다.

명령프롬프트를 관리자의 권한으로 시작합니다.



관련 폴더로 이동합니다.



서명 명령어는 다음과 같습니다.

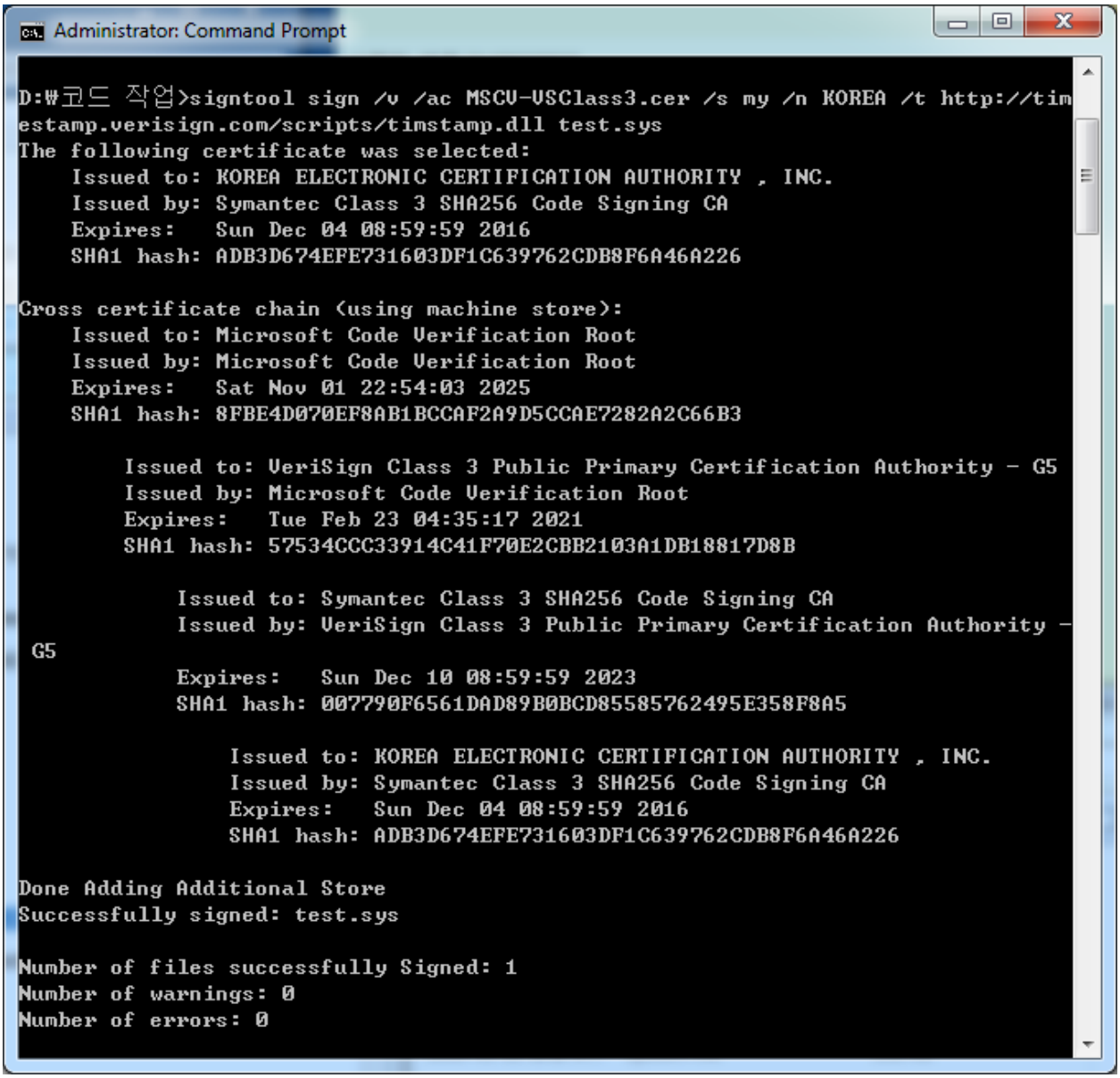
signtool sign /v /ac MSCV-VSClass3.cer /s my /n (회사명) /t http://timestamp.verisign.com/scripts/timstamp.dll (파일명)

(/n (회사명) : 회사명 입력시 전체이름의 앞부분만 입력(공백 입력시 Error)

(ex. KOREA ELECTRONIC CERTIFICATION AUTHORITY , INC. -> 'KOREA' 로 입력)

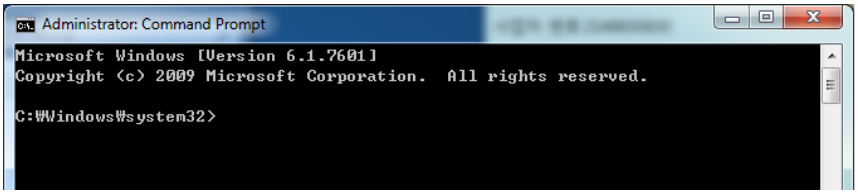
서명 명령어의 예시입니다.

signtool sign /v /ac MSCV-VSClass3.cer /s my /n KOREA /t http://timestamp.verisign.com/scripts/timstamp.dll test.sys



2.3 Dual sign

명령프롬프트를 관리자의 권한으로 시작합니다.



관련 폴더로 이동합니다.

서명 명령어는 다음과 같습니다.

서명순서는 sha1먼저 그리고 sha2입니다.

SHA-1

signtool.exe sign /f cert.pfx /p (비밀번호) /d (설명) /du (배포url) /fd sha1 /t http://timestamp.verisign.com/scripts/timstamp.dll (서명할파일명)

SHA-2

signtool.exe sign /f cert.pfx /p (비밀번호) /as /d (설명) /du (배포url) /fd sha256 /tr http://sha256timestamp.ws.symantec.com/sha256/timestamp (서명할파일명)

서명 명령어의 예시입니다.

SHA-1

signtool.exe sign /f cert-sha1.pfx /p 1234 /d Test /du http://www.test.com /fd sha1 /t http://timestamp.verisign.com/scripts/timstamp.dll test.cab

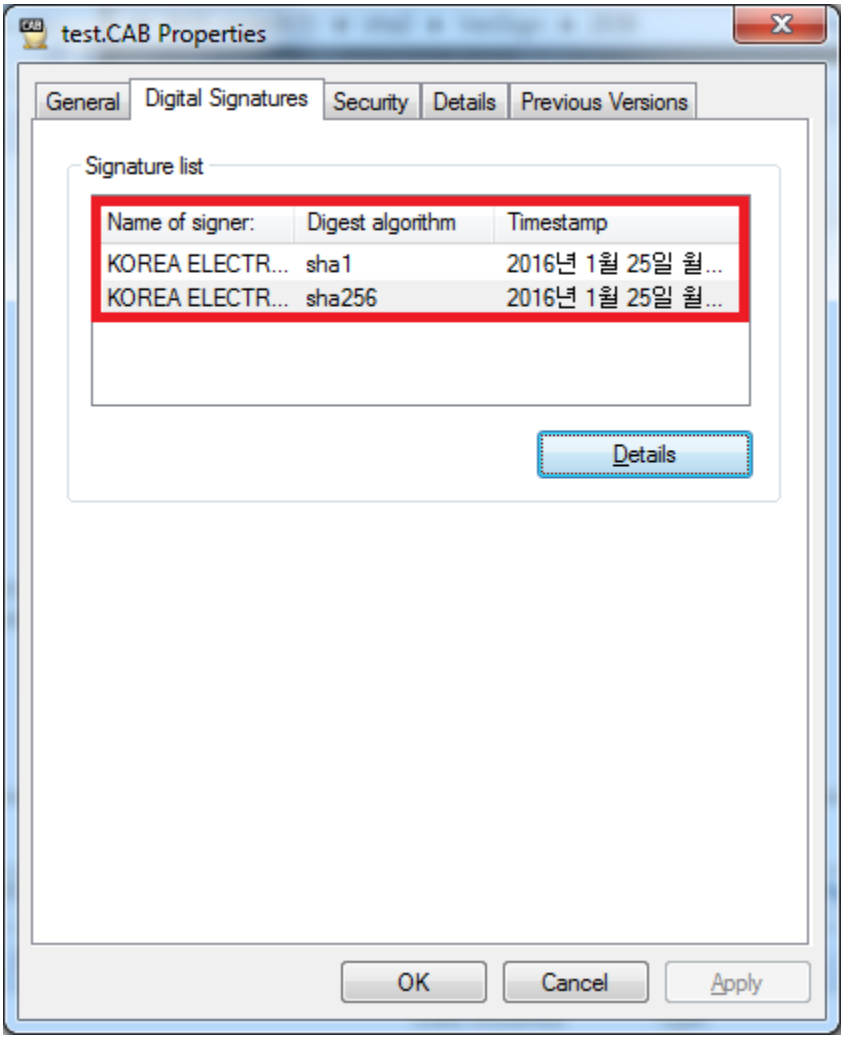
SHA-2

signtool.exe sign /f cert-sha2.pfx /p 1234 /as /d Test /du http://www.test.com /fd sha256 /tr http://sha256timestamp.ws.symantec.com/sha256/timestamp /td sha256 test.cab

```
E:₩SignTool>signtool.exe sign /f cert-sha1.pfx /p 1234 /d Test /du http://www.te
st.com /fd sha1 /t http://timestamp.verisign.com/scripts/timstamp.dll test.cab
Done Adding Additional Store
Successfully signed: test.CAB

E:₩SignTool>signtool.exe sign /f cert-sha2.pfx /p 1234  /as /d Test /du http://w
ww.test.com /fd sha256 /tr http://timestamp.geotrust.com/tsa /td sha256  test.ca
b
Done Adding Additional Store
Successfully signed: test.CAB
```

마우스 우클릭하여 속성을 클릭한 후 보이는 화면

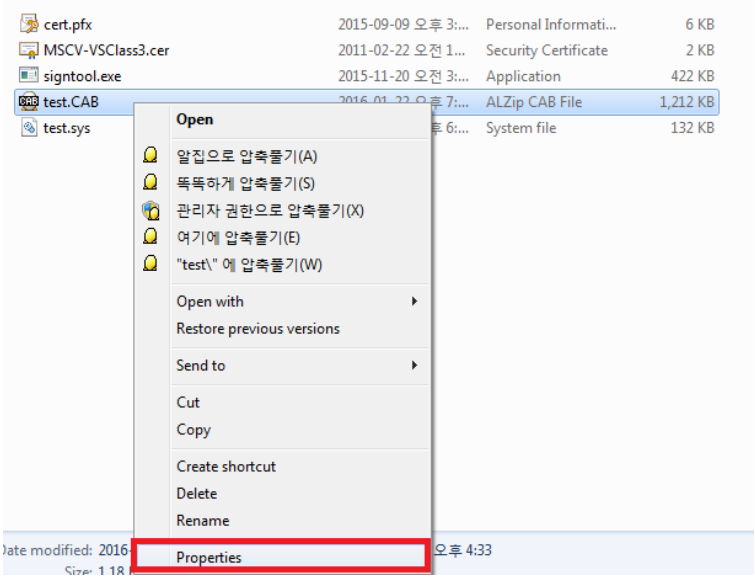


두 개의 서명이 모두 있는 것을 확인 할 수 있습니다.

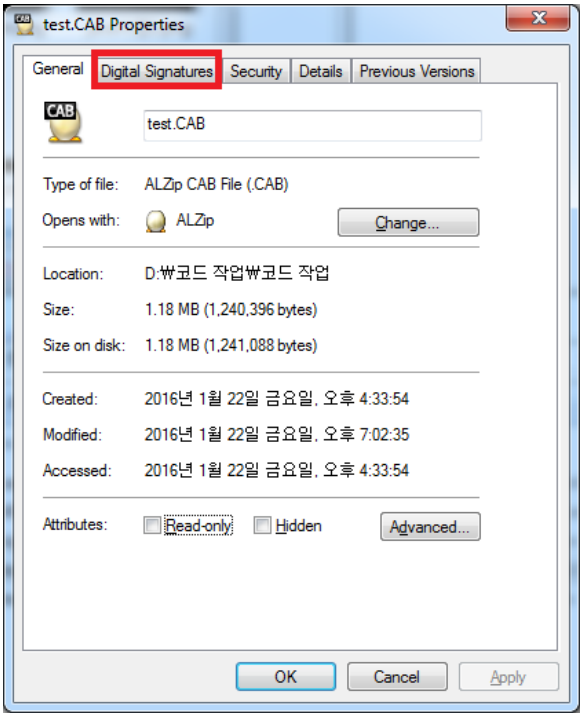
자세한 확인은 2.4정상 서명 확인 방법에 나와있습니다.

2.4 정상 서명 확인 방법

윈도우 환경에서 확인하는 방법

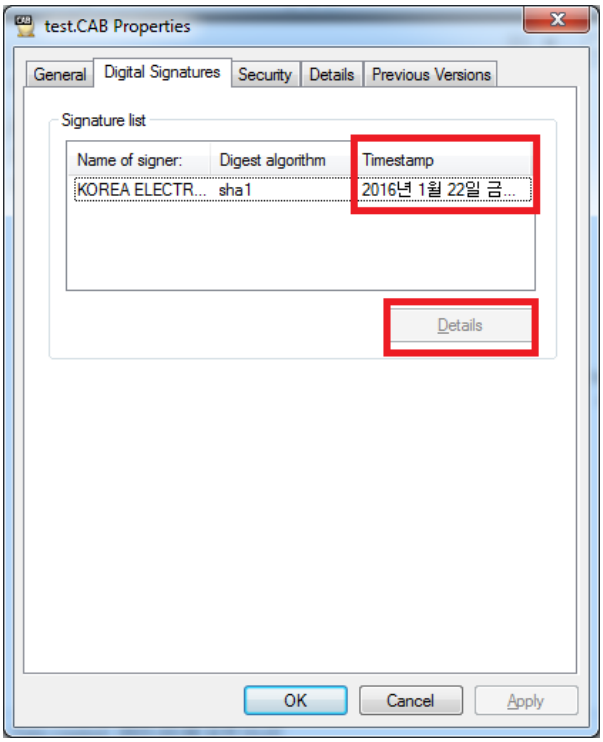


서명된 파일을 마우스 우 클릭 하여 메뉴를 열어서 마지막 속성을 선택합니다.



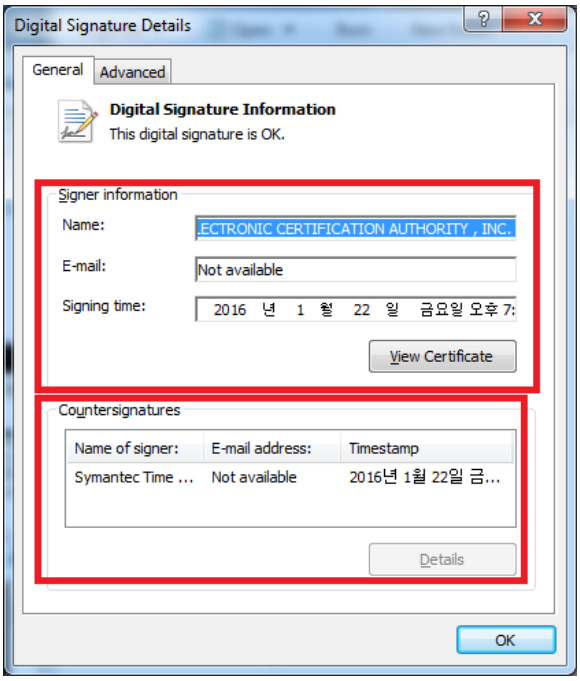
정상 서명이 되었다면 디지털 서명 탭이 생성이 되어 있습니다.

(서명된 이후에 생성되는 탭입니다)



타임스탬프 옵션이 적용되었다면 관련 창에 서명 날짜가 보여집니다.

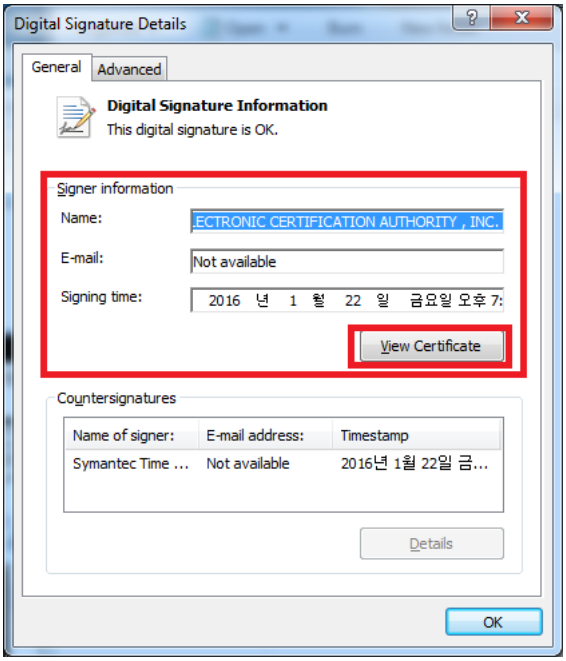
날짜가 있다면 타임스탬프 옵션이 적용되었습니다.



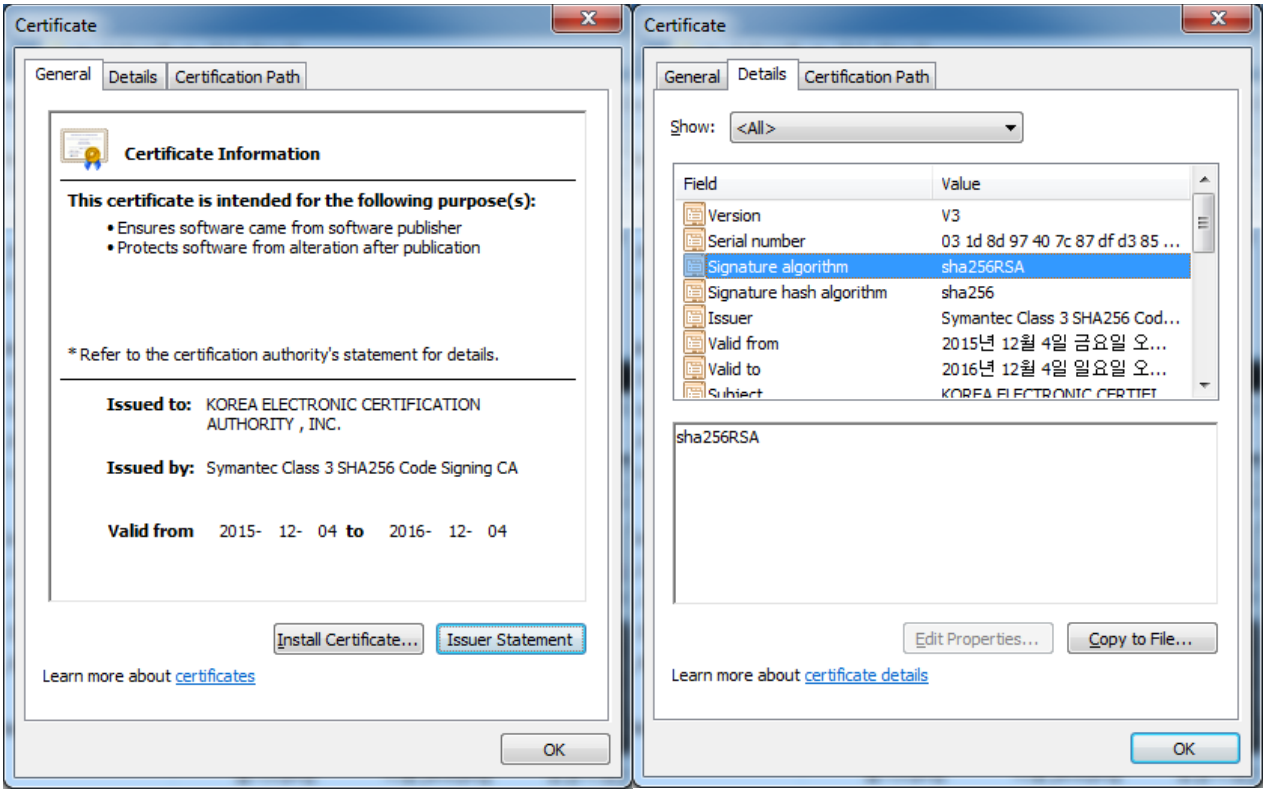
서명된 인증서와 서명된 타임스탬프 인증서의 정보를 볼 수 있습니다.

듀얼 서명의 경우 각각의 인증서를 하나씩 확인하시기 바랍니다.

서명된 인증서 확인하기



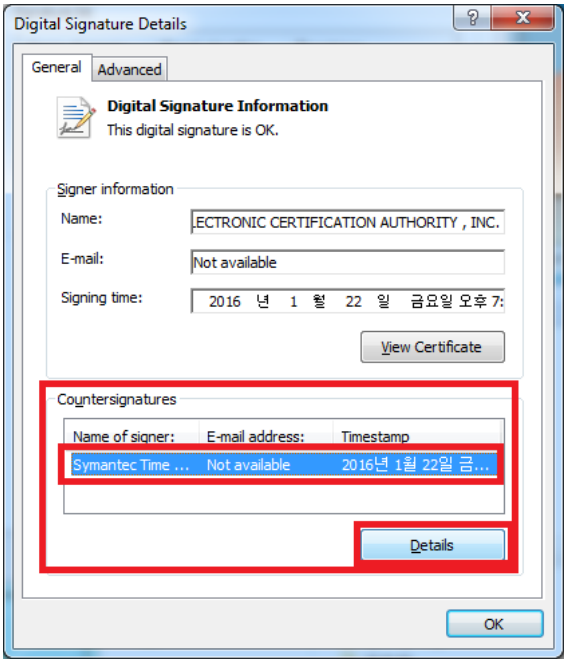
인증서보기를 선택합니다.



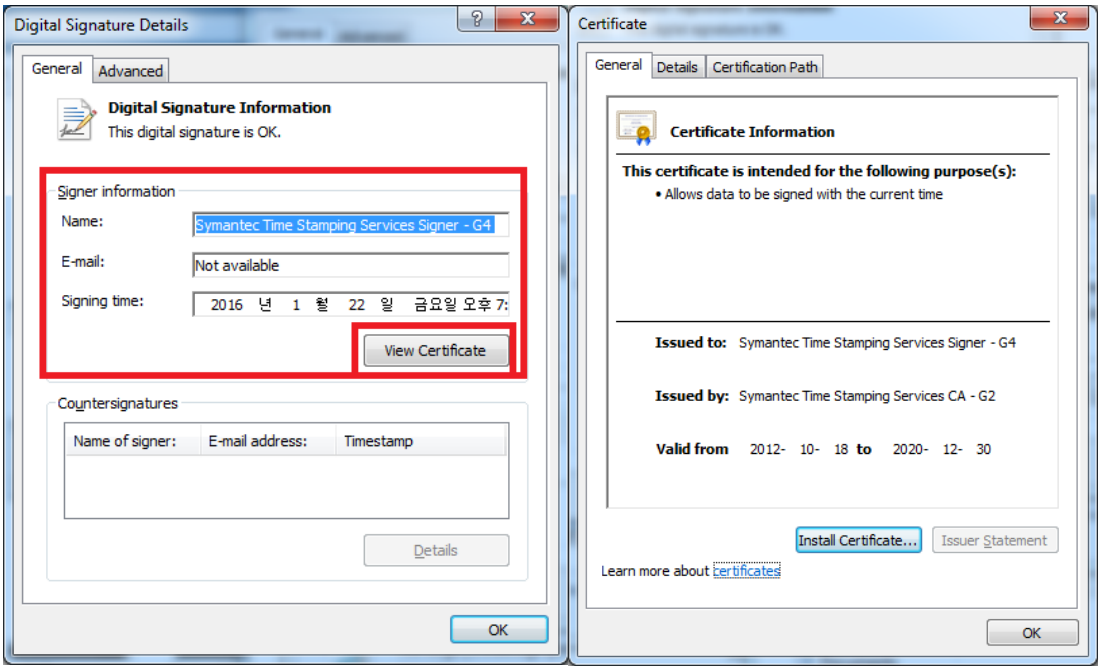
해당 인증서 정보를 확인할 수 있습니다.

보여지는 인증서의 자세히 탭으로 들어가면 인증서 알고리즘을 확인할 수 있습니다.

타임스탬프 인증서 확인하기



교차서명상의 인증서를 선택하고 자세히를 누릅니다.



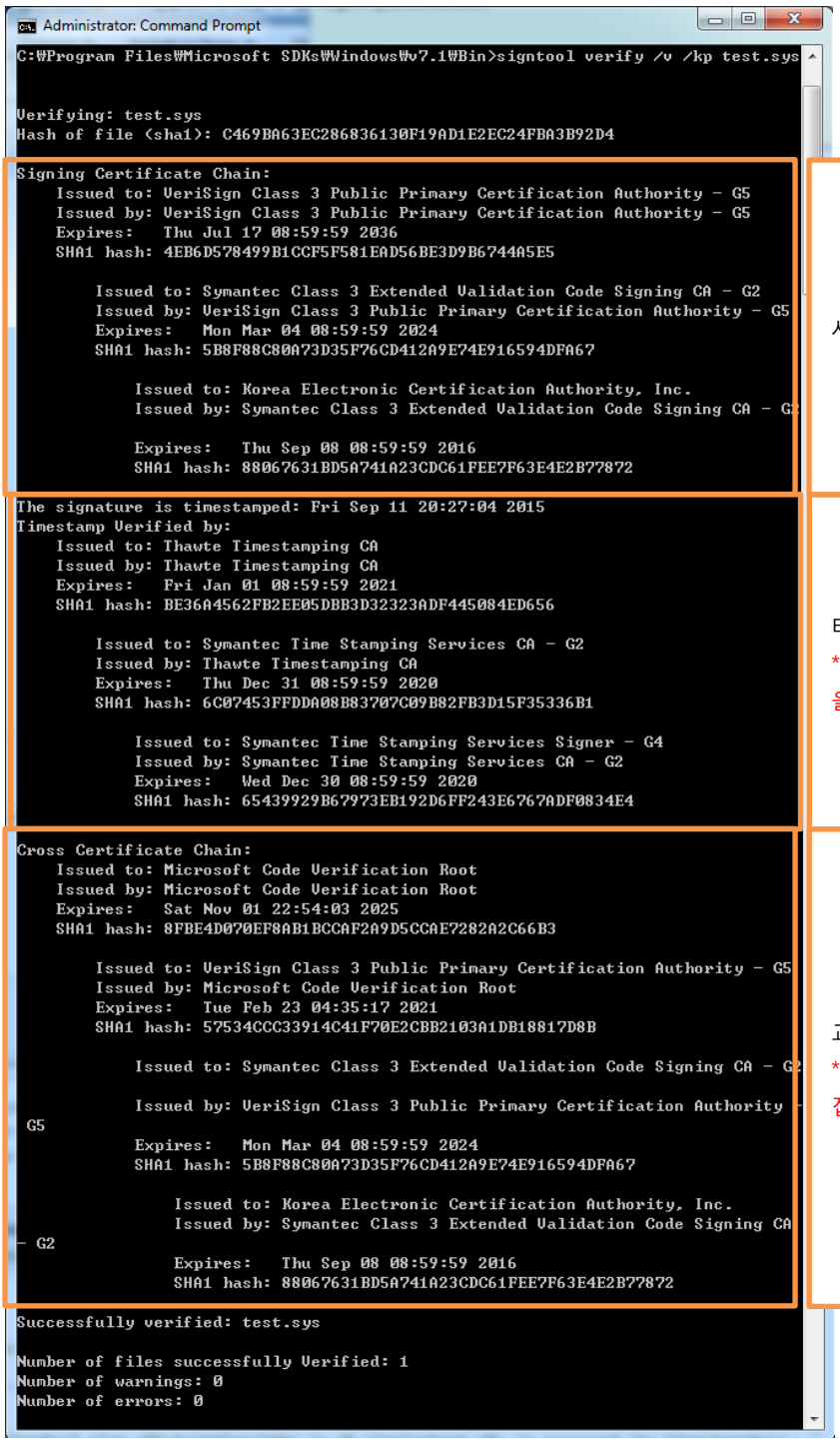
인증서 보기를 누르시면 타임스탬프 인증서 정보를 확인할 수 있습니다.

타임스탬프 옵션을 준 인증서의 경우 파일의 유효기간은 타임스탬프 인증서의 유효기간과 같습니다.

명령어로 확인하는 방법.

Signtool verify /v /kp (파일명)

정상적으로 서명이 진행되었다면 다음과 화면처럼 나타나게 됩니다.



서명한 인증서에 대한 정보입니다.

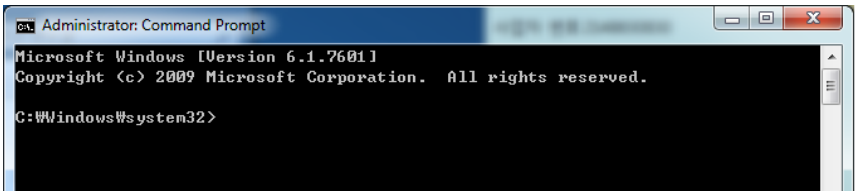
타임스탬프 인증서에 대한 정보입니다.
*타임스탬프 옵션을 사용하여 서명 했을 때에만 보여집니다.

교차서명 인증서에 대한 정보입니다.
*교차서명으로 서명 했을 때에만 보여집니다.

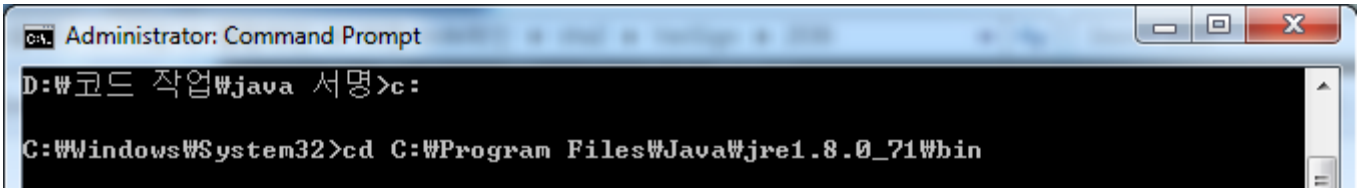
3. Java

3.1 Java Sign

명령프롬프트를 관리자의 권한으로 시작합니다.



관련 폴더로 이동합니다.



서명 명령어는 다음과 같습니다.

jarsigner -storetype pkcs12 -keystore cert.p12 -tsa http://timestamp.geotrust.com/tsa 서명할파일명.jar alias

서명 명령어의 예시입니다.

jarsigner -storetype pkcs12 -keystore cert.p12 -tsa http://timestamp.geotrust.com/tsa test.jar alias

3.2 Java 정상 서명 확인하기

정상서명 확인 명령어입니다.

jarsigner -verify -verbose -certs [서명된 jar파일]

서명 확인 명령어의 예시입니다.

jarsigner -verify -verbose -certs test.jar

```
C:₩Program Files₩Java₩jdk1.8.0_71₩bin>jarsigner -verify -verbose -certs test.jar
```

다음과 같은 화면이 출력됩니다.

4. code관련 이슈 정리

일반적으로 sha1이슈로 sha2로 변경되는 경우 다음과 같은 이슈가 발생됩니다.

1. 기존 sha1인증서 sha2로 재발급 하는 경우

-예상되는 문제점은 다음과 같습니다.

윈도우 2003,XP에서 패치 안된 클라이언트의 호환성문제로 인식 못하는 클라이언트가 발생 될 수 있습니다

윈도우 2003,XP를 사용하는 고객의 패치가 필요합니다

응용프로그램이 스마트스크린 필터에 걸립니다.

2. 기존 sha1인증서를 사용하고 sha2인증서를 새로 받는 경우

Vista이하 버전에서는 sha1사용 7이상에서 sha2사용(권장)

듀얼 서명으로 sha1,sha2를 한 파일에 모두 서명

응용프로그램이 스마트스크린 필터에 걸립니다.

3. 기존 sha1인증서를 사용하고 EV인증서를 새로 받는 경우

-Vista 이하 버전에서는 sha1서명 사용 7이상에서 EV사용

Sha1에서 sha2로 변경 시 주의 사항에 대하여 알려드립니다.

재발급은 기존 sha1이 폐기되고 sha2로 나가는 형식입니다.(기존 인증서 만료와는 다릅니다.)

파일에 타임스탬프 작업이 되어 있다 하더라도 모든 배포 파일에 신규 인증서로 재 서명 작업이 진행되어야 합니다.

또한 응용 프로그램의 경우에는 스마트스크린 필터 문제가 생깁니다.

새로 받은 인증서는 인증서 평판이 구축이 안되어 있습니다(기존인증서의 경우는 평판구축이 완료되어 있습니다)

기존 인증서에서 안 걸리던 스마트 스크린필터가 신규 인증서에서는 걸리게 되어 있습니다

새로운 인증서로 서명된 파일이 스마트스크린 필터에서 안 걸리는 경우는 EV인증서만 입니다

평판이 구축되는 동안 스마트 스크린필터를 꺼주시거나 EV인증서를 받으셔야 합니다.

(윈도우 패치나 스마트 스크린필터를 끄는 작업은 모두 접속되는 클라이언트(다운받으시는 고객 측)에서 작업되어야 합니다)

Signtool.exe 설치 실패 관련 오류

기존 visual studio나 .net framework와 충돌이 생길 경우 완료된 것처럼 보이나 롤백 되어 관련 폴더나 파일이 없는 경우가 있습니다.

기존 프로그램을 삭제하거나 깨끗한 환경에서 설치하시어 서명작업을 부탁 드립니다.

기존 pvk, spc파일이 없는 이유

기존 signcode.exe의 경우 hash알고리즘의 선택이 md5,sha1으로만 선택 가능합니다.

Signtool의 경우 sha256옵션이 선택 가능한 강력한 툴입니다.

기존에는 어떤 툴을 사용하든 상관이 없어서 두 가지 툴에서 사용되는 형식 모두를 보내드렸습니다.

보안 권고상 signcode에서 사용되던 pvk,spc파일이 빠지고 signtool 용 pfx파일만 나가게 됩니다.

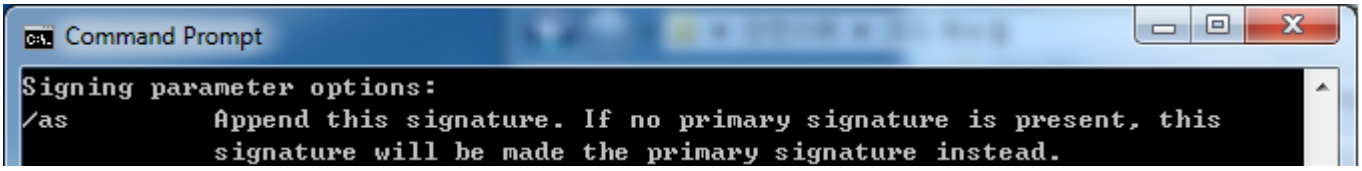
듀얼 서명 시 /as 관련 에러가 나는 경우

해당 signtool의 버전이 낮아서 발생됩니다.

Signtool sign /? 명령어 실행 시 옵션 중 /as가 있어야 합니다.

서명 전 /as 옵션이 있는지 확인을 바랍니다.

없다면 최신버전으로 다시 받으시기 바랍니다.



화면과 같은 옵션 설명이 있어야 합니다.

(윈도우 8.1이나 10용 SDK에서 관련 옵션이 활성화 되어 있습니다)

타임스탬프 옵션

인증서의 유효기간은 해당 인증서로 서명작업을 진행할 수 있는 기간을 말합니다

보통 서명된 파일의 유효기간은 인증서를 따라갑니다.

타임스탬프 옵션이 적용된 파일의 유효기간은 타임스탬프 인증서의 유효기간을 따라갑니다.

해당 기간의 확인 방법은 2.4의 서명 확인하기를 보시면 됩니다.

/fd sha256 옵션

현재 이슈가 되고 있는 sha1,sha2이슈와는 다릅니다.

배포 파일 서명에 사용되는 hash알고리즘의 선택입니다.

현재 가장 강력한 옵션이 /fd sha256입니다(권장)

Windows Xp,2003에서는 /fd sha256으로 설정하면 정상적으로 보이지 않습니다.

해당 os에서는 /fd sha1을 사용하시기 바랍니다.

Sha1인증서를 계속 쓸 수 있나요?

현재 sha1인증서를 사용 할 수 있는 os는 Windows XP, Vista, 2003제품군입니다.

Windows 7이상에서는 무조건 sha2를 사용하여야 합니다.

예외적으로 SHA1인증서로 서명이 되었다 하더라도 2015년 12월 31일 이전에 타임스탬프 옵션이 적용된 파일은 계속 사용이 가능합니다.

다만 패치나 다른 수정사항으로 인하여 재 서명이 되어야 한다면 sha2 인증서로 서명되어야 합니다.

한국전자인증 기술지원팀 Tel : 02-1588-1314(3) / Fax : 02-2055-3732
E-Mail : cs@crosscert.com