코드서명 검증모듈 개발자 가이드

□ 개요

o 이 문서는 한국인터넷진흥원이 MicroSoft사의 WindowsTM 환경에서 코드서명된 모듈을 검증하기 위한 라이브러리API에 대한 설명을 포함하고 있습니다.

- 본 제품은 PC에서의 웹 하드, 백신, 기타 설치 프로그램 등 전용 사용자 프로그램을 이용하는 서비스의 경우 소프트웨어(SW)설치 및 업데이트 시 악성코드를 유포하는 경우 코드서명 여부 및 게시자 확인을 할 수 있도록 하여 신뢰성 검증을 수행하기 위함입니다.

- 본 제품은 소프트웨어(SW) 배포자 인증 및 무결성을 제공하는 코드서명 기술을 이용, 전용 프로그램의 악성코드 유포 방지 방안을 마련하고자 합니다.

- 이 문서는 제공되는 각 프로그램 및 모듈의 API에 대한 사용 방법과 환경 구성에 대한 가이드를 포함하고 있으며 제품 버전에 따른 문서 내용이 달라질 수 있습니다

- 코드서명 검증 Toolkit 관련 모듈 구성

구성	내용
WinTrustDll.dll	모듈 및 프로그램의 코드서명 여부를 검증을 수행하는 DLL 모듈
wintrustDll_Sample	코드서명 모듈 검증 Sample 프로그램 (Visual C++ 6.0)

o 코드사인 인증서는 베리사인(VeriSign), 써트(Thawte), 금융결제원(yessign)에서 발급하고 있으며 발급기관 홈페이지에 코드서명 방법이 기술되어 있습니다.

- 베리사인 및 써트 코드서명 인증서 : 국내 한국전자인증, 써트코리아에서 발급 대행

※ 발급 관련 홈페이지 : http://www.crosscert.com, https://www.certkorea.co.kr

o yessign 코드서명 인증서

- 국내 공인인증기관인 금융결제원에서 발급

※ 발급 관련 홈페이지 : https://www.yessign.or.kr/ssl/index.htm

※ 코드서명 생성 가이드 문서는 발급기관 홈페이지를 이용하시기 바랍니다.

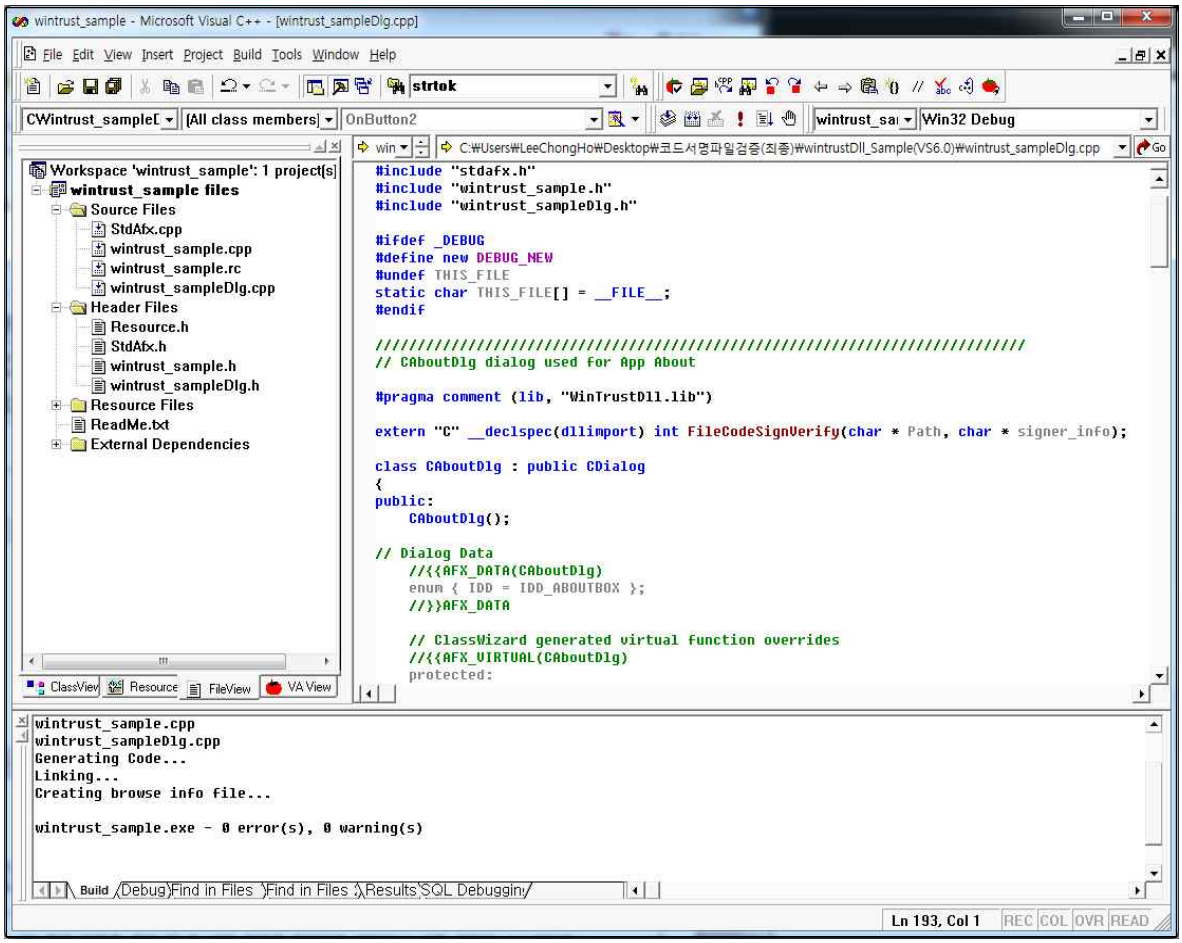
o 코드서명을 하기 위해서는 다음과 같은 구성이 되어야 합니다.

- .SPC(코드서명 인증서 파일), .PVK(코드서명 인증서 개인키 파일)
- 코드서명 생성 프로그램(예 : signcode.exe, codesign.bat, ...등)
- chktrust.exe : 코드서명 결과를 확인하는 프로그램
- 코드서명할 파일 : CAB, EXE, DLL, OCX, ...등

□ 환경구성

o 본 제품은 코드서명된 파일 및 모듈에 대해 검증을 수행하며 코드서명을 하기 전 실행파일 및 업데이트 파일 소스코드 내에 API를 적용하여 사용할 수 있습니다. 다음은 소스코드 적용 방법에 대해 설명하고 있습니다.

- wintrustDll_Sample
- WinTrustDll.dll에서 제공되는 API를 적용한 샘플 프로그램입니다.
- DLL 연동이 가능한 모든 개발언어를 지원 합니다. (C++, C#, PB, ...)
- 본 설명 문서는 Visual Studio 6.0에서 개발된 샘플 프로그램입니다.
- API 적용 방법을 확인 한 후 실제 배포용 업데이트 파일이나 실행 파일의 소스코드에 적용 합니다.
- 파일서명 검증 : 검증 대상 경로 내 지정된 파일만 검증 합니다.




```
void CWintrust_sampleDlg::OnButton1()
{
    // TODO: Add your control notification handler code here
    int result_value = 0;
    CString temp;

    result_value = FileCodeSignVerify("C:₩₩atioglxx.dll", "(주)제이엔티시스템");
//  result_value = FileCodeSignVerify("C:₩₩atioglxx.dll", "KOSCOM");
//  result_value = FileCodeSignVerify("C:₩₩SKCommIF.dll", "KOSCOM");
//  result_value = FileCodeSignVerify("C:₩₩SKCommAX.ocx", "KOSCOM");

    temp.Format("%d", result_value);
    AfxMessageBox(temp);

}
```

- 배포 관련 : 신규 설치 시 WinTrustDll.dll만 배포합니다. (레지스트리 등록 절차 없음)

□ 코드서명 검증 함수

o FileCodeSignVerify

- 기능 : 모듈에 대한 코드서명 여부를 검증 하는 함수
- 함수 : int FileCodeSignVerify(char * FilePath, char * signer_info)
- 인자값

  char * FilePath : 검증 대상 모듈 Full 경로(모듈명 및 확장자 포함)

  Char * signer_info : 서명자 명 입력
- 반환값 : 해당 모듈에 대해 코드서명 여부 및 체인 검증 수행 후 해당 코드를 반환

□ 반환값 및 에러코드

o 코드서명 파일 검증 에러 코드

0	:	정상 코드서명
-1	:	서명되지 않았습니다
-2	:	신뢰되지 않은 인증서및 인증 기관 입니다.
-3	:	알 수 없는 공급자입니다.
-4	:	신뢰할 수 없는 사용자의 인증서
-5	:	신뢰할 수 없는 발급자 명
-6	:	암호화 실패
-7;	:	기타 에러

o 체인검증 관련 에러 코드

1000	:	코드 서명 및 체인 검증 성공
1001	:	인증서 유효기간이 만료 되었습니다.
1002	:	인증서 또는 체인 인증서가 폐지 되었습니다.
1003	:	인증서 또는 체인 인증서의 전자서명이 유효하지 않습니다.
1004	:	인증서 또는 체인 인증서의 사용 용도가 적합하지 않습니다.

1005 : 신뢰할 수 없는 최상위 기관 입니다.

1006 : 인증서 또는 체인 인증서의 폐지 상태를 알 수 없습니다.

1007 : 체인인증서 내의 인증서가 초기 인증서를 인증 했던 인증기관에 의해 발급 되었습니다.

1008 : 인증서 체인이 완료 되지 않았습니다.

1009 : 체인을 생성하는데 사용한 CTL이 유효하지 않습니다.

1010 : 체인을 생성하는데 사용한 CTL의 전자서명이 없습니다.

1011 : 체인을 생성하는데 사용하기 적합한 CTL이 아닙니다.

1012 : 서명자 정보와 게시자 정보가 일치 하지 않습니다.

-101 : 서명 정보 생성 실패

-102 : 인증서 컨텍스트 읽기 실패

-103 : 게시자 정보 길이 추출 실패

-104 : 게시자 정보 값 추출 실패

-105 : 발급자 정보 길이 추출 실패

-106 : 발급자 정보 값 추출 실패

-107 : 인증서 저장소 내 다음 인증서 컨텍스트 읽기 실패

-108 : 서명자 정보 길이 추출 실패

-109 : 서명자 정보 값 추출 실패

-1000 : 체인 인증서 목록 생성 실패