

软件安全—恶意代码机理与防护

3.9 PE文件的数字签名与验证机制

杨秀璋

武汉大学国家网络安全学院

1455136241@qq.com



3.9 PE文件的数字签名与验证机制

- PE文件的数字签名过程及验证机制
 - 签名数据解析-以Zoomit为例
-

3.9.1 PE文件的数字签名过程及验证机制

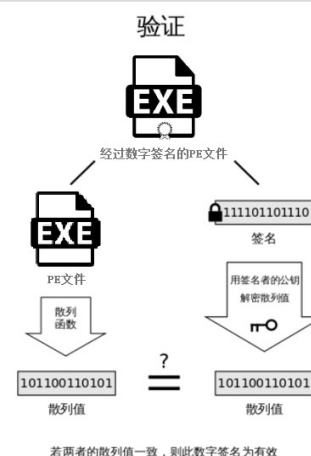
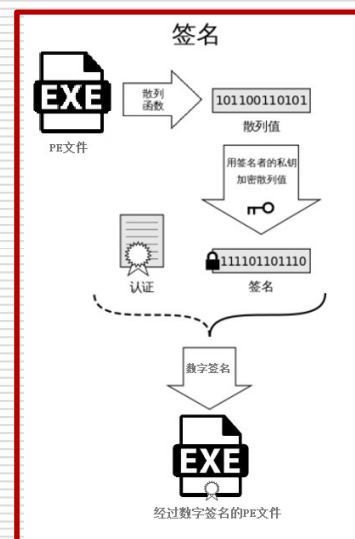
□ 对PE文件进行数字签名的作用

- 防篡改：通过对数字签名的验证，保证文件未被非法篡改。
 - 降低误报：安全软件通过验证文件是否有正规厂商的数字签名来降低误报。
-

PE文件的数字签名过程

□ PE文件是怎样被签名的

- 软件发布者使用散列算法（如MD5或SHA）计算PE文件的散列值。
- 软件发布者使用私钥对散列值进行签名得到签名数据。
- 将签名私钥对应的公钥和签名数据等以证书的形式附加在PE文件之中，形成经过数字签名的PE文件。
- 软件发布者将经过数字签名的PE文件进行发布。



PE文件签名位置

- 对哪些数据签名？
- 签名数据放在哪里？
 - Certificate Table: PE文件可选文件头DataDirecotry第5项（文件偏移及大小）

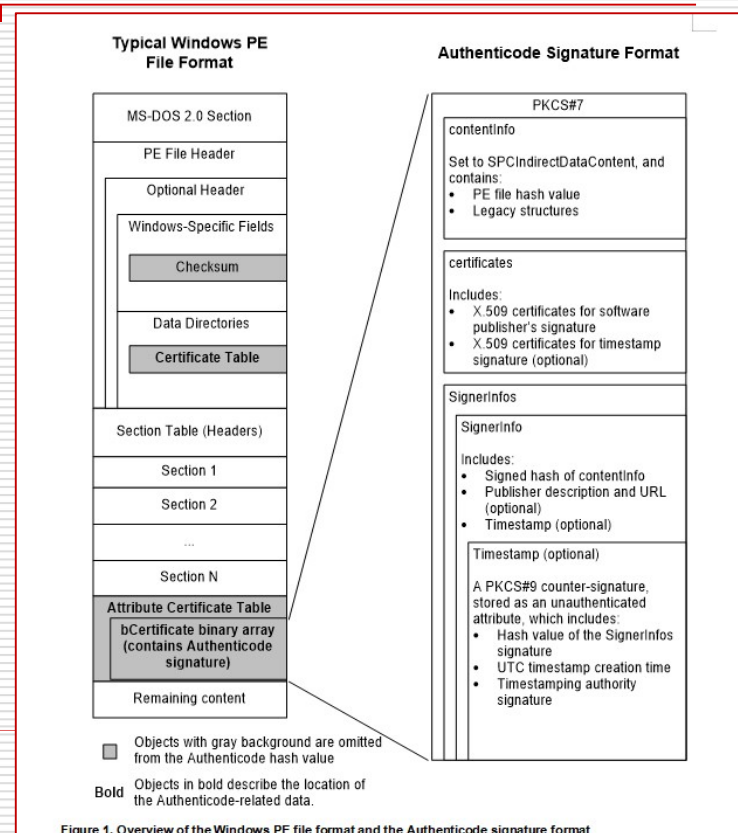
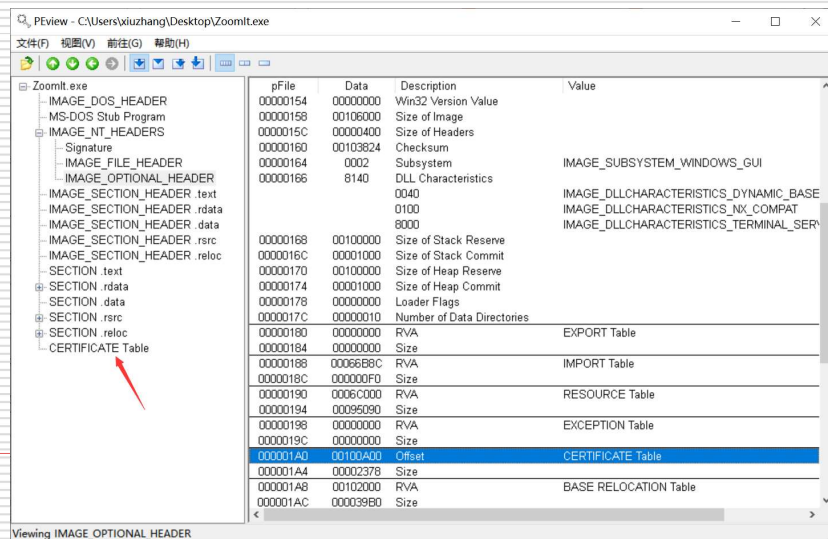
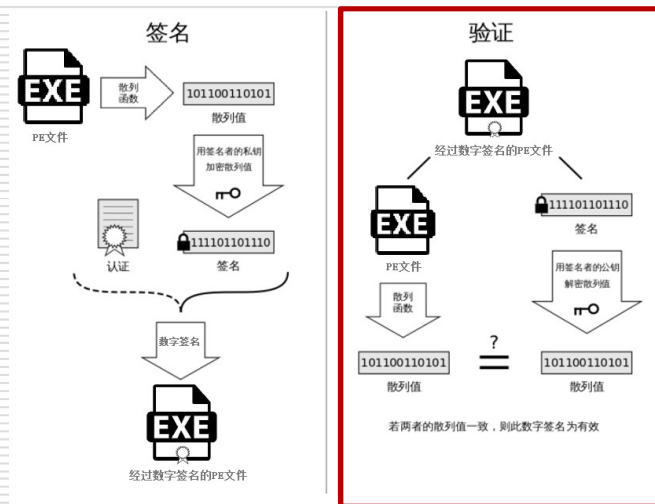


Figure 1. Overview of the Windows PE file format and the Authenticode signature format

PE文件的签名验证机制

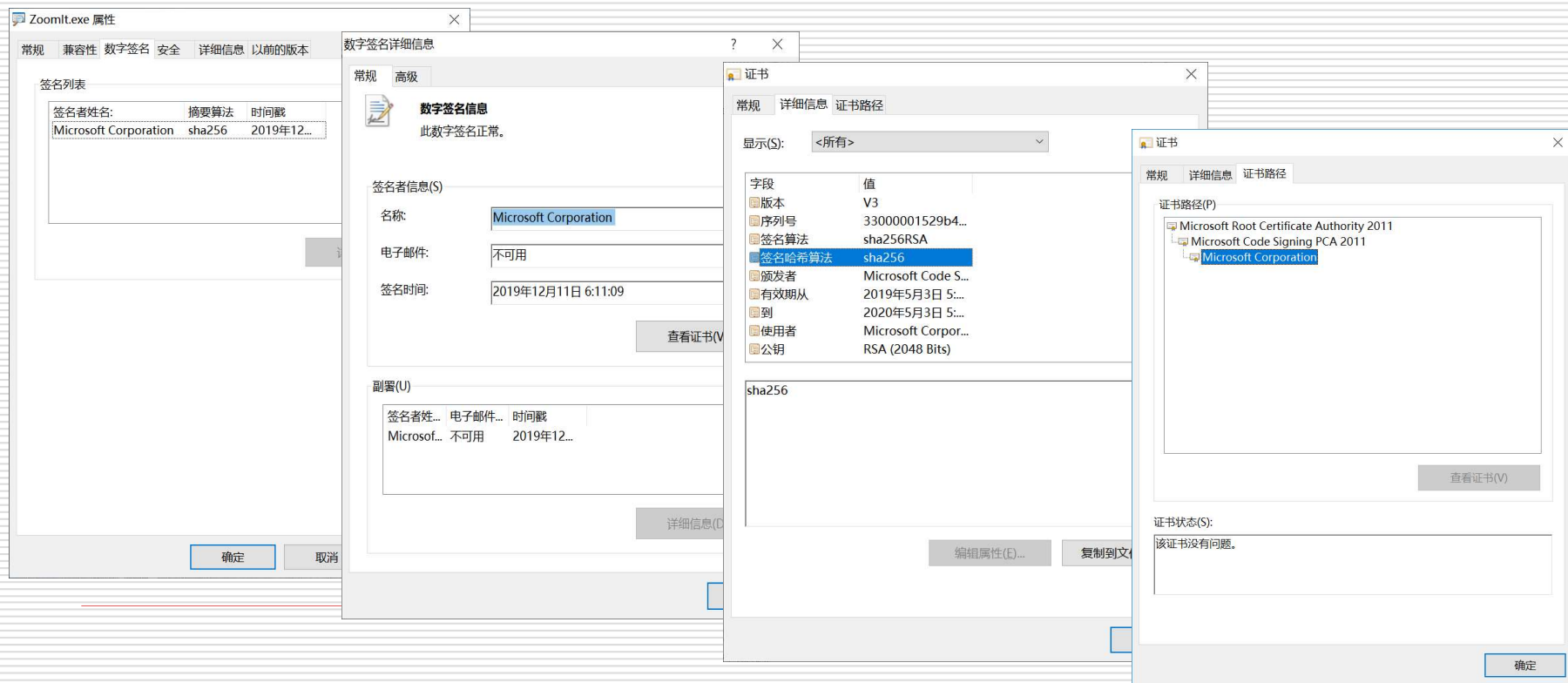
□ 当软件使用者获得**PE**文件后，系统如何进行验证呢？

- 从**PE**文件证书中提取软件发布者的公钥、使用的散列算法、签名算法、原始散列值的签名数据。
- 使用提取的公钥和对应签名验证算法将签名数据还原为原始**PE**文件的原始散列值。
- 对现有**PE**文件使用同样的散列算法计算出对应的散列值。
- 对比两个散列值是否一致，从而判断数据是否被破坏和篡改。



另外，系统还将验证证书路径和时间戳，以确保被验证**PE**文件的软件发布方身份和签名时间的可靠性。

3.9.2 Zoomit签名数据解析



zoomit签名数据解析

- 文件开始位置：00100A00（长度：2378H）
 - 表项长度：4字节，头部和签名数据的总长度
 - 证书版本：2字节，常见0x0200表示WIN_CERT_REVISION_2
 - 证书类型：2字节，常见0x0002表示包含PKCS#7的SignData结构
 - SignedData**：包含PE文件Hash值的**签名数据**、软件发布者公钥，选用的**签名及散列算法**等。（在文件中为ASN.1编码）

PEView - C:\Users\Earnest\Desktop\Zoomit.exe

	RVA	Data	Description	Value
Zoomit.exe				
IMAGE_DOS_HEADER	00000154	00000000	Win32 Version Value	
MS-DOS Stub Program	00000158	00106000	Size of Image	
IMAGE_NT_HEADERS	0000015C	00000400	Size of Headers	
Signature	00000160	00103825	Checksum	
IMAGE_FILE_HEADER	00000164	0002	Subsystem	
IMAGE_OPTIONAL_HEADER	00000166	8140	DLL Characteristics	
IMAGE_SECTION_HEADER.text	00000168	00100000	Size of Stack Reserve	
IMAGE_SECTION_HEADER.rdata	0000016C	00001000	Size of Stack Commit	
IMAGE_SECTION_HEADER.data	00000170	00100000	Size of Heap Reserve	
IMAGE_SECTION_HEADER.rsrc	00000174	00001000	Size of Heap Commit	
IMAGE_SECTION_HEADER.reloc	00000178	00000000	Loader Flags	
SECTION.text	0000017C	00000010	Number of Directories	
SECTION.rdata	00000180	00000000	RVA	EXPORT Table
SECTION.data	00000184	00000000	Size	
SECTION.rsrc	00000188	00066B8C	RVA	IMPORT Table
SECTION.reloc	0000018C	000000F0	Size	
	00000190	0006C000	RVA	RESOURCE Table
	00000194	00095090	Size	
	00000198	00000000	RVA	EXCEPTION Table
	0000019C	00000000	Size	
	000001A0	00100A00	RVA	CERTIFICATE Table
	000001A4	00002378	Size	

PEView - C:\Users\xiuzhang\Desktop\Zoomit.exe

	pFile	Raw Data	Value
Zoomit.exe			
IMAGE_DOS_HEADER	00100A00	78 23 00 00 00 02 00 00	30 82 23 68 06 09 2A 86 x#.....0.#k...*
MS-DOS Stub Program	00100A10	48 B6 F7 0D 01 07 02 A0	82 23 5C 30 82 23 58 02 H.....#%0.#X...
IMAGE_NT_HEADERS	00100A20	01 01 31 0F 30 0D 06 09	60 B6 48 01 65 03 04 02 .1.0...#.He...
IMAGE_SECTION_HEADER.text	00100A30	01 05 00 30 5C 06 0A 2B	06 01 04 01 82 37 02 01 ...0V...+...7...
IMAGE_SECTION_HEADER.rdata	00100A40	04 A0 4E 30 4C 30 17 06	0A 2B 06 01 04 01 82 37 ...N0L0...+...7...
IMAGE_SECTION_HEADER.data	00100A50	02 01 0F 30 09 03 01 00	A0 04 A2 02 80 00 30 31 ...0...H...e...01
IMAGE_SECTION_HEADER.rsrc	00100A60	30 0D 06 09 60 B6 48 01	65 03 04 02 01 05 00 04 ...#.He...e...01
IMAGE_SECTION_HEADER.reloc	00100A70	20 2C E4 12 EC 94 72 C9	0B 25 54 BF C0 50 8D 35 ...r...%T...].5
SECTION.text	00100A80	26 EB 7A 73 80 0F 7F D4	C1 EC 55 11 25 8D CA 96 &.zs...U...%...
SECTION.rdata	00100A90	44 A0 82 0D 85 30 82 06	03 30 82 03 EB A0 03 02 D...0...0...0...
SECTION.data	00100AA0	01 02 02 13 33 00 00 01	52 9B 40 9F 50 56 99 75 ...3...R@PV.u...
SECTION.rsrc	00100AB0	88 00 00 00 00 01 52 30	0D 06 09 2A 86 48 86 F7 ...R0...*.H...
SECTION.reloc	00100AC0	0D 01 01 0B 05 00 30 7E	31 0B 30 09 06 03 55 04 ...0~1.0...U...
	00100AD0	06 13 02 55 53 31 13 30	11 06 03 55 04 08 13 0A ...UST1.0...U...
	00100AE0	57 61 73 68 69 6E 67 74	6F 6E 31 10 30 0E 06 03 Washington1.0...
	00100AF0	55 04 07 13 07 52 65 64	6D 6F 6E 64 31 1E 30 1C U...Redmond1.0...
	00100B00	06 03 55 04 0A 13 15 4D	69 63 72 6F 73 6F 66 74 ...U...Microsoft
	00100B10	20 43 6F 72 70 6F 72 61	74 69 6F 6E 31 28 30 26 Corporation1(0&...
	00100B20	06 03 55 04 03 13 1F 4D	69 63 72 6F 73 6F 66 74 ...U...Microsoft
	00100B30	20 43 6F 64 65 20 53 69	67 6E 69 6E 67 20 50 43 Code Signing PC
	00100B40	41 20 32 30 31 31 30 1E	17 0D 31 39 30 35 30 32 A 20110...190502
	00100B50	32 31 33 37 34 36 5A 17	0D 32 30 30 35 30 32 32 213746Z...2005022
	00100B60	31 33 37 34 36 5A 30 74	31 0B 30 09 06 03 55 04 13746Z011.0...U...
	00100B70	06 13 02 55 53 31 13 30	11 06 03 55 04 08 13 0A ...UST1.0...U...

zoomit签名数据解析

①指定SignedData结构

PKCS#7

1.2.840.113549.1.7.2

②生成签名的哈希算法

MD5 1.2.840.113549.2.5

SHA1 1.3.14.3.2.26

SHA256 2.16.840.1.101.3.4.2.1

③签名属性

SPC 1.3.6.1.4.1.311.2.1.4

ASN.1 Dump Utility

File Edit Options Help

File: C:\Users\Xiuzhang\Desktop\ZoomIt02.dat

Time: 22:24:10, 03/08/2020

```
0 30 9067: SEQUENCE {
  4 06 9: OBJECT IDENTIFIER signedData (1 2 840 113549 1 7 2)
  15 A0 9052: [0] {
    19 30 9048: SEQUENCE {
      23 02 1: INTEGER 1
      26 31 15: SET {
        28 30 13: SEQUENCE {
          30 06 9: OBJECT IDENTIFIER '2 16 840 1 101 3 4 2 1'
          41 05 0: NULL
        }
      }
    }
  }
  43 30 92: SEQUENCE {
    45 06 10: OBJECT IDENTIFIER
    57 A0 78: spcIndirectDataContext (1 3 6 1 4 1 311 2 1 4)
    59 30 76: [0] {
      61 30 23: SEQUENCE {
        63 06 10: OBJECT IDENTIFIER
        75 30 9: spcPcmImageData (1 3 6 1 4 1 311 2 1 15)
        77 03 1: SEQUENCE {
          BIT STRING 0 unused bits
          Error: Object has zero length.
        }
      }
    }
  }
  80 A0 4: [0] {
    82 A2 2: [2] {
```

Authenticode Signature Format

PKCS#7

contentInfo

Set to SPCIndirectDataContent, and contains:

- PE file hash value
- Legacy structures

certificates

Includes:

- X.509 certificates for software publisher's signature
- X.509 certificates for timestamp signature (optional)

SignerInfos

SignerInfo

Includes:

- Signed hash of contentInfo
- Publisher description and URL (optional)
- Timestamp (optional)

Timestamp (optional)

A PKCS#9 counter-signature, stored as an unauthenticated attribute, which includes:

- Hash value of the SignerInfos signature
- UTC timestamp creation time
- Timestamping authority signature

PE文件数字签名解析

```
ASN.1 Dump Utility
File Edit Options Help
175 30 13: SEQUENCE {
177 06 9:   OBJECT IDENTIFIER '1 2 840 113549 1 1 11'
188 05 0:   NULL
190 30 126: }
192 31 11: SEQUENCE {
194 30 9:   SET {
196 06 3:     SEQUENCE {
201 13 2:       OBJECT IDENTIFIER countryName (2 5 4 6)
                PrintableString 'US'
                }
                }
205 31 19:   }
207 30 17:   SEQUENCE {
209 06 3:     OBJECT IDENTIFIER stateOrProvinceName (2 5 4 8)
214 13 10:    PrintableString 'Washington'
                }
226 31 16:   SET {
228 30 14:     SEQUENCE {
230 06 3:       OBJECT IDENTIFIER localityName (2 5 4 7)
235 13 7:        PrintableString 'Redmond'
                }
                }
244 31 30:   SET {
246 30 28:     SEQUENCE {
248 06 3:       OBJECT IDENTIFIER organizationName (2 5 4 10)
253 13 21:        PrintableString 'Microsoft Corporation'
                }
                }
276 31 40:   SET {
278 30 38:     SEQUENCE {
280 06 3:       OBJECT IDENTIFIER commonName (2 5 4 3)
285 13 31:        PrintableString 'Microsoft Code Signing PCA 2011'
                }
                }
ASN.1 Dump complete: 22:24:10, 03/08/2020 with 2 warnings, 7 errors.
```

证书颁发者信息

①OID值

②国家名称

③州或省名称

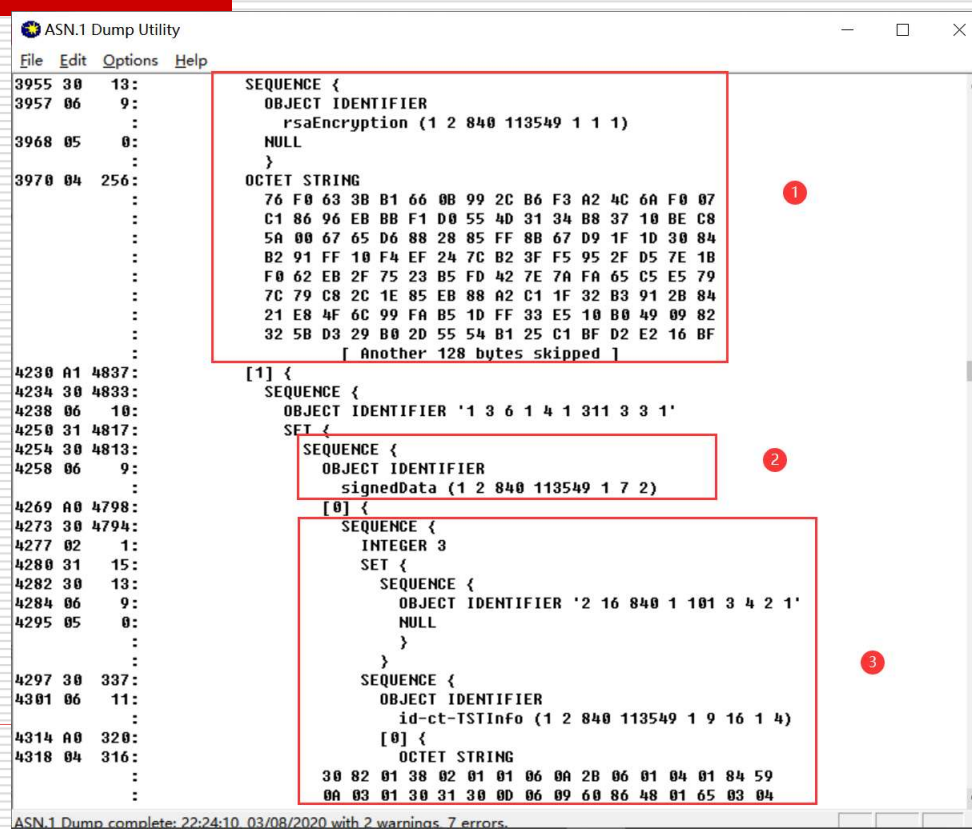
④城市名称

⑤组织名称

⑥通用名

验证证书链相关字段:

- ❑ ①签名算法：RSA加密
- ❑ ②signedData采用PKCS#7格式
- ❑ ③SHA256散列算法



PE文件数字签名解析

❑ 散列算法：SHA256

```
SEQUENCE {  
  OBJECT IDENTIFIER '2 16 840 1 101 3 4 2 1'  
  NULL  
}
```

❑ 摘要数据

```
SEQUENCE {  
  OBJECT IDENTIFIER  
    messageDigest (1 2 840 113549 1 9 4)  
  SET {  
    OCTET STRING  
      FF A8 29 9B 70 AD 5B 35 BD BE C9 5F 21 33 63 84  
      95 80 DA 45 F6 22 F0 CD 8D 74 1A 7A 2B 44 08 A1  
  }  
}
```

❑ 公钥数据

```
SEQUENCE {  
  OBJECT IDENTIFIER  
    rsaEncryption (1 2 840 113549 1 1 1)  
  NULL  
}  
BIT STRING 0 unused bits  
30 82 01 0A 02 82 01 01 00 B1 A7 89 D3 F6 A7 EE  
F4 ED 74 88 9C 9E C1 85 C7 94 DF 96 12 1E FD 36  
8A 2B F6 78 4C E9 E9 D4 35 B0 9B 85 7F 6F 4B EF  
1C FF 77 88 55 AC D2 62 75 41 4E A2 F3 5B BC 56  
37 56 C2 70 8B 43 6E C1 33 28 41 36 06 CC 12 BA  
7E C9 F7 10 9A 2F 07 06 1C A1 6B FA A5 94 97 3E  
E1 87 D4 5C 9A 36 12 90 E1 8D C9 B3 9F AE 08 F7  
B2 6D 03 4A DA 0A F2 58 F0 13 25 15 79 17 CC 1F  
[ Another 142 bytes skipped ]  
}
```

❑ RSA签名后的数据

```
SEQUENCE {  
  OBJECT IDENTIFIER '1 2 840 113549 1 1 11'  
  NULL  
}  
OCTET STRING  
B0 DE FB 7B 7D 26 28 FE 5B A6 D9 A4 DB E7 F6 BE  
17 C6 EC 7D E5 8B 1D 0D DD 6D BF 5E 2A 27 AA 64  
64 28 CF B2 98 1F D8 21 24 3E 27 86 18 6A EC 3D  
C0 09 23 4D 66 3B A4 57 03 9A 21 6D BD C6 A8 DB  
8B 26 4D 2A 2A FD 4A 5C 0C 68 0A 9C 6F 9C 8B 53  
78 AA 88 A2 65 6C 0A A2 F9 EA 50 EA 5C C4 4C 44  
59 39 41 CC 71 94 29 FB 1E 5B 4F 65 6F B0 12 4C  
D6 11 11 B2 EB E3 45 04 9B B5 29 08 44 6F 32 04  
[ Another 128 bytes skipped ]
```