Public Key Management

HW5 - CNS Sapienza

Andrea Fioraldi 1692419

2018-11-30

1 Introduction

There are many different encoding and structures for public and private keys. We present an overview about the formats using the most widespreads Public-Key Cryptography Standards [1] versions.

2 DER Encoding

DER (Distinguished Encoding Rules) is the most popular of the ASN.1 [2] encodings.

The encoding of an object follows this structure:

1. Identifier octets
2. Length octets
3. Contents octets
4. End-of-contents octets

Complex data structures can be binary-encoded following this structure (you can for example convert any data stired in JSON).

DER is widely used in cryptography to encode the data structures exposed in the following section.

A DER file has usually the extension `.der` and contains only the binary data encoded using such format.

3 PEM Files

PEM (Privacy-Ehanced Mail) is a standard file format for storing keys and it was introduced in [3]. It is used for both public and private keys. PEM encode this binary information using base64 and so it is an ASCII format.

The structure is quite simple:

1. Header: `-----BEGIN` type of cryptographic data `-----`;
2. Encoded base64 data, generally encoded with DER;
3. Footer: `-----END` type of cryptographic data `-----`;

Usually, the extension of a PEM file is `.pem`.

Here an example file of an RSA public key:

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA3gmCqlQvCaE9eR31msxo
mM0lJarQf0/kkxAFVmXuLlOXsCt3Nroj3qs58CadPRh4kBg+4KgegkXzaQ8EVIAE
eI4WRR3Ku3dVdX8+i7bNuFGlgoSgpIOgAk4s7SNxRWuoUMTIAg1sxpvYzYeTyDdT
2PjWjkZ3H7M2V3TPoVw9GLoIur0l6Z96vp1LXWX4acocvCZRKLltPQAZiB5c9hXc
kKhNcRWde/5gopv7qyYxxzPQqU4spKID6afNDMsJ9ldK18YQcQvnjo4mIIoQdvFT
i7BJLtxhURQjp5CcZrwFT2Fj3V9MNfYS5yRi/fx17ZMlCAFZLbFVwEK7vLdywyZA
3QIDAQAB
-----END PUBLIC KEY-----
```

4 Data structures

Public and Private keys are stored using different data structures. We present the most used structures from the Public-Key Cryptography Standards.

4.1 PKCS#1

It is the RSA Cryptography Standard defined in [4]. It defines the ASN.1 encoding of RSA public and private keys.

The DER structure of a public key is the following:

```
RSAPublicKey ::= SEQUENCE {
    modulus           INTEGER,  -- n
    publicExponent    INTEGER   -- e
}
```

The structure of a private key is:

```
RSAPrivateKey ::= SEQUENCE {
  version           Version,
  modulus           INTEGER,  -- n
  publicExponent    INTEGER,  -- e
  privateExponent   INTEGER,  -- d
  prime1            INTEGER,  -- p
  prime2            INTEGER,  -- q
  exponent1         INTEGER,  -- d mod (p-1)
  exponent2         INTEGER,  -- d mod (q-1)
  coefficient       INTEGER,  -- (inverse of q) mod p
  otherPrimeInfos   OtherPrimeInfos OPTIONAL
}
```

4.2 PKCS#7

It is the Cryptographic Message Syntax Standard defined in [5]. It is usually employes in Public Keys infrastructures.

An associated file extesion is `.p7b` when using a PEM file containing data structured following the PKCS#7 specification.

The DER structure of both public and provate key is based on the following structure:

```
RecipientInfo ::= SEQUENCE
{
    version                 INTEGER,
    issuerAndSerialNumber   IssuerAndSerialNumber,
    keyEncryptionAlgorithm  KeyEncryptionAlgId,
    encryptedKey            EncryptedKey
}
```

The set of structures that can be chained is large and it is explained in a short summary by Microsoft [6].

4.3 PKCS#12

It is one of the complex formats for storing cryptographical objects.

An associated file extesion is `.pfx` or `.p12` and they are archives containing data structured following the PKCS#12 specification.

One of the major novelties of this format is that the content can be encrypted in a surgical way in containers calles "SafeBags".

The definition of the structures [7] is very complex and it was criticized for this in the past.

4.4 A note on encrypted Private Keys

It is a commom practice to encrypt the private keys using a simmetric algorithm. The most used are AES and 3-DES. The previous exposed formats stores fields in order to recognize if a key is crypted and wich algorithm was used.

References

[1] *PKCS - Wikipedia.*
`https://en.m.wikipedia.org/wiki/PKCS` Accessed: 2018-12-6.

[2] *Abstract Syntax Notation One - Wikipedia.*
`https://en.wikipedia.org/wiki/Abstract_Syntax_Notation_One` Accessed: 2018-12-6.

[3] *RFC 7468.*
`https://tools.ietf.org/html/rfc7468` Accessed: 2018-12-6.

[4] *RFC 8017.*
`https://tools.ietf.org/html/rfc8017` Accessed: 2018-12-6.

[5] *RFC 2315.*
`https://tools.ietf.org/html/rfc2315` Accessed: 2018-12-6.

[6] *PKCS — Microsoft Docs.*
`https://docs.microsoft.com/en-us/windows/desktop/seccertenroll/pkcs--7-attribu` Accessed: 2018-12-6.

[7] *RFC 7292 - Page 10.*
`https://tools.ietf.org/html/rfc7292#page-10` Accessed: 2018-12-6.