¿Que dice aca?

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

```
Tm9zLCBsb3MgcmVwcmVzZW50YW50ZXMgZGVsIHB1ZWJsbyBkZSBsYSBOYWNp824g
QXJnZW50aW5hLCByZXVuaWRvcyBlbiBDb25ncmVzbyBHZW5lcmFsIENvbnN0aXR1
eWVudGUgcG9yIHZvbHVudGFkIHkgZWxlY2Np824gZGUgbGFzIHByb3ZpbmNpYXMg
cXVlIGxhIGNvbXBvbmVuLCBlbiBjdW1wbGltaWVudG8gZGUgcGFjdG9zIHByZWV4
aXN0ZW50ZXMsIGNvbiBlbCBvYmpldG8gZGUgY29uc3RpdHVpciBsYSB1bmnzbiBu
YWNpb25hbCwgYWZpYW56YXIgbGEganVzdGljaWEsIGNvbnNvbGlkYXIgbGEgcGF6
IGludGVyaW9yLCBwcm92ZWVyIGEgbGEgZGVmZW5zYSBjb236biwgcHJvbW92ZXIg
ZWwgYmllbmVzdGFyIGdlbmVyYWwsIHkgYXNlZ3VyYXIgbG9zIGJlbmVmaWNpb3Mg
ZGUgbGEgbGliZXJ0YWQgcGFyYSBub3NvdHJvcywgcGFyYSBudWVzdHJhIHBvc3Rl
cmlkYWQgeSBwYXJhIHRvZG9zIGxvcyBob21icmVzIGRlbCBtdW5kbyBxdWUgcXVp
ZXJhbiBoYWJpdGFyIGVuIGVsIHN1ZWxvIGFyZ2VudGlubzsgaW52NhbmRvIGxh
IHByb3RlY2Np824gZGUgRGlvcywgZnVlbnRlIGRlIHRvZGEgcmF6824geSBqdXN0
aWNpYTogb3JkZW5hbW9zLCBkZWNyZXRhbW9zIHkgZXN0YWJsZWNlbW9zIGVzdGEg
Q29uc3RpdHVjafNuIHBhcmEgbGEgTmFjafNuIEFyZ2VudGluYS4gCg==
```

Base64

- **Mecanismo de codificación que utiliza un conjunto de 64 caracteres para codificar cualquier valor posible de un byte. Toma 3 bytes, y los convierte en 4. Usa A-Z,a-z,0-9,+,/ e = para el padding**

Ej: "**Mensaje en claro**"

Codificado en base 64:

TWVuc2FqZSBlbiBjbGFybwo=

MIME

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

- **Multipurpose Internet Mail Extensions (MIME) es un estándar de internet (rfc 2045 y sigs.) que extiende el formato de los emails para soporta texto en sets de caracteres distintos al US-ASCII, binarios anexados, mensajes que incluyan distintos tipos de objetos. Los tipos de contenidos definidos por MIME son muy utilizados en otros protocolos como por ejemplo HTTP.**

Ejemplos de Content-type

- text
  - text/plain
  - text/richtext
- message
  - message/rfc822
- image
  - image/jpeg
  - image/gif
- video
  - video/mpeg
- application
  - application/PostScript
  - application/octet-stream
- multipart
  - multipart/mixed
  - multipart/alternative

S/MIME

- **S/MIME (Secure / Multipurpose Internet Mail Extensions) es un estándar para cifrado de clave pública y firma de emails. Define el content-type application/pkcs7…**

- **La funcionalidad de S/MIME está implementada en la mayoría de los clientes de correo electrónico.**

Servicios Provistos por S/MIME

- **Autoria**
- **Integridad del mensaje**
- **No repudio**
- **Confidencialidad de los datos**

ASN.1 (Abstract Syntax Notation 1)

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

- **Establece una sintaxis abstracta para la definición de estructuras independientemente de la arquitectura de hardware o lenguaje de implementación.**
- **Utilizado en la definición de estructuras de datos para intercambio de aplicaciones.**
- **Tipos de datos:**
  - SEQUENCE, SET, CHOICE, OBJECT IDENTIFIER, BIT STRING, OCTET STRING, INTEGER, UTCTime

ASN.1 (Abstract Syntax Notation 1)

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

- **Ejemplos**

```
Certificate ::=  SEQUENCE {
   tbsCertificate        TBSCertificate,
   signatureAlgorithm    AlgorithmIdentifier,
   signatureValue        BIT STRING  }

TBSCertificate  ::=  SEQUENCE  {
   version       [0]  EXPLICIT Version DEFAULT v1,
   serialNumber       CertificateSerialNumber,
   signature          AlgorithmIdentifier,
   issuer             Name,
   ...
```

ASN.1 (Abstract Syntax Notation 1)

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

- **Ejemplos**

```
Version ::= INTEGER { v1(0), v2(1), v3(2) }

Validity ::= SEQUENCE {
   notBefore      Time,
   notAfter       Time }

Time ::= CHOICE {
   utcTime        UTCTime,
   generalTime    GeneralizedTime }
```

OID (Object Identifier)

- **Código de identificación única de un objeto o estructura.**
- **Componen una estructura jerárquica.**
- **Existe un registro internacional de OIDs.**
- **Se utilizan para la identificación de:**
  - Atributos
  - Extensiones
  - Algoritmos
  - Politicas de Certificación
  - Estructuras de datos
  - ...

OID (Object Identifier)

- **Algunos OIDs asignados:**

Atributos estándar

```
id-at OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) ds(5) 4}
```

Extensiones estándar

```
id-ce OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) ds(5) 29}
```

OID (Object Identifier)

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

- **Algunos OIDs asignados:**

Atributos estándar

```
id-at OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) ds(5) 4}
id-at-name       AttributeType ::= { id-at 41 }
id-at-surname    AttributeType ::= { id-at 4 }
id-at-givenName  AttributeType ::= { id-at 42 }
id-at-initials   AttributeType ::= { id-at 43 }
id-at-commonName AttributeType ::= { id-at 3 }
```

OID (Object Identifier)

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

- **Tipos de representación**

```
commonName ::= { 2 5 4 3 }
commonName ::=   2.5.4.3
commonName ::= { id-at 3 }

id-at OBJECT IDENTIFIER ::= {joint-iso-ccitt(2) ds(5) 4}
```

- **Procedimiento para obtenerlos**
  - Registro frente al IANA (http://www.iana.org)
  - En Argentina, el nodo 2.16.32 lo administra la Secretaría de Gabinete y Gestión Pública. (http://www.jgm.gov.ar/sgp/paginas.dhtml?pagina=134)

Codificación (Encoding Rules)

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

- **Establecidos por ITU-T en X.690.**
- **Definen una representación concreta de datos a utilizar para almacenar o transferir información.**
- **Son utilizados para la representación de los datos definidos por ASN.1**

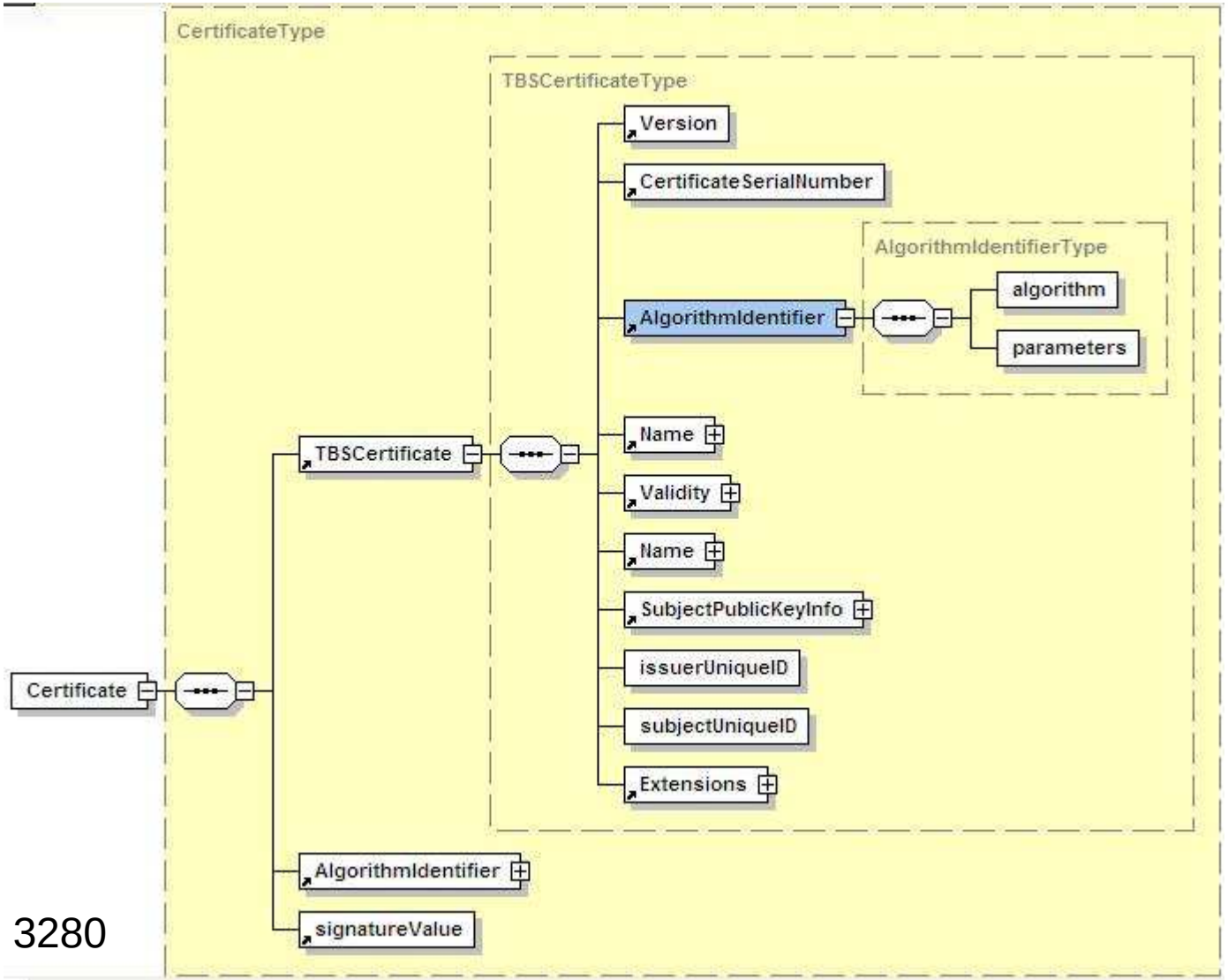
- **Existen distintos tipos reglas de codificación:**
  - BER : Basic Encoding Rules
  - CER : Canonical Encoding Rules
  - DER : Distinguished Encoding Rules
  - PER : Packed Encoding Rules

Codificación (Encoding Rules)

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

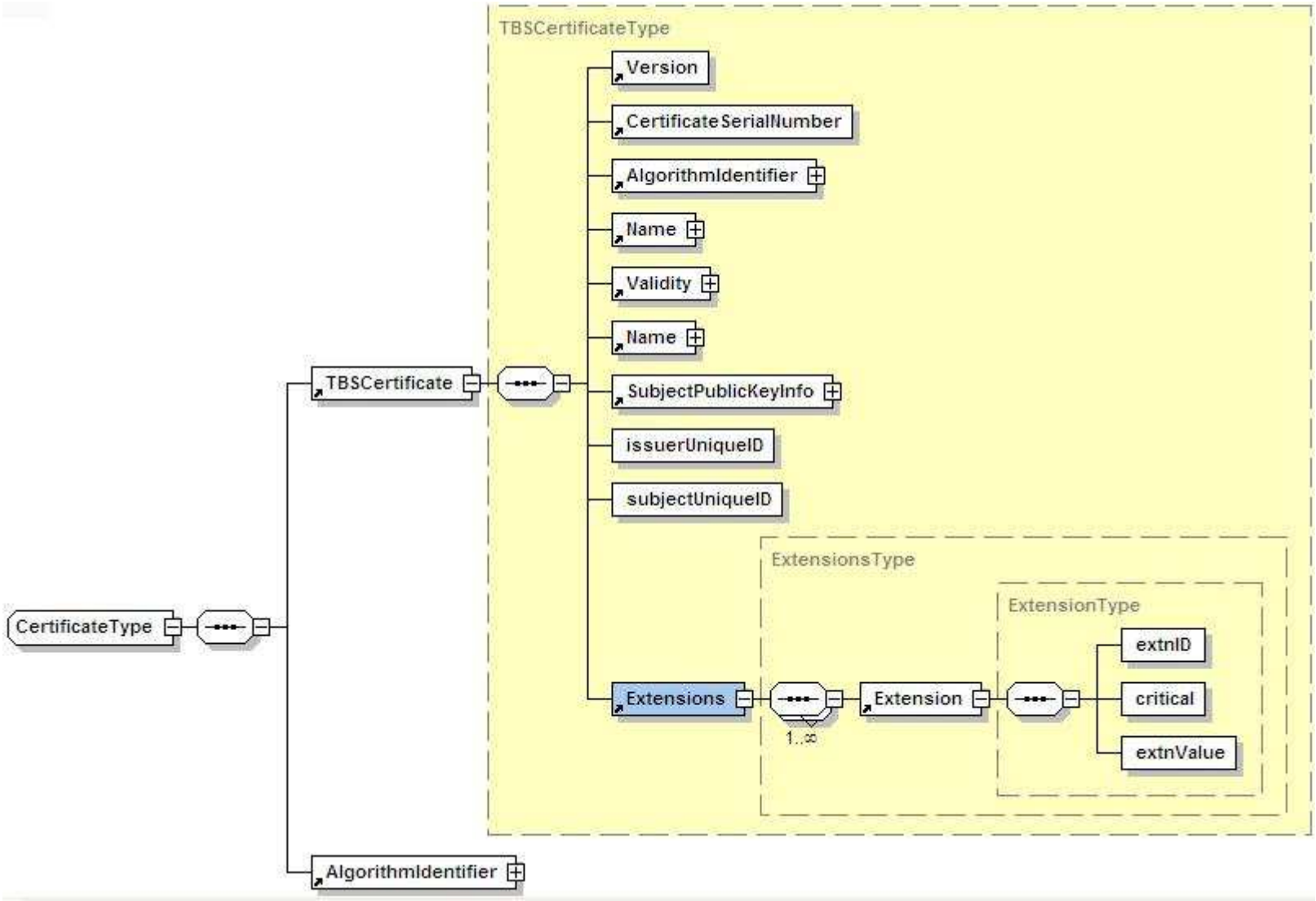
- **Códigos de tipos de datos**
  - 02_{16} **INTEGER**
  - 03_{16} **BIT STRING**
  - 04_{16} **OCTET STRING**
  - 05_{16} **NULL**
  - 06_{16} **OBJECT IDENTIFIER**
  - 30_{16} **SEQUENCE**
  - 31_{16} **SET**
  - $A0_{16}$ **CONTEXT SPECIFIC**

Certificados X.509

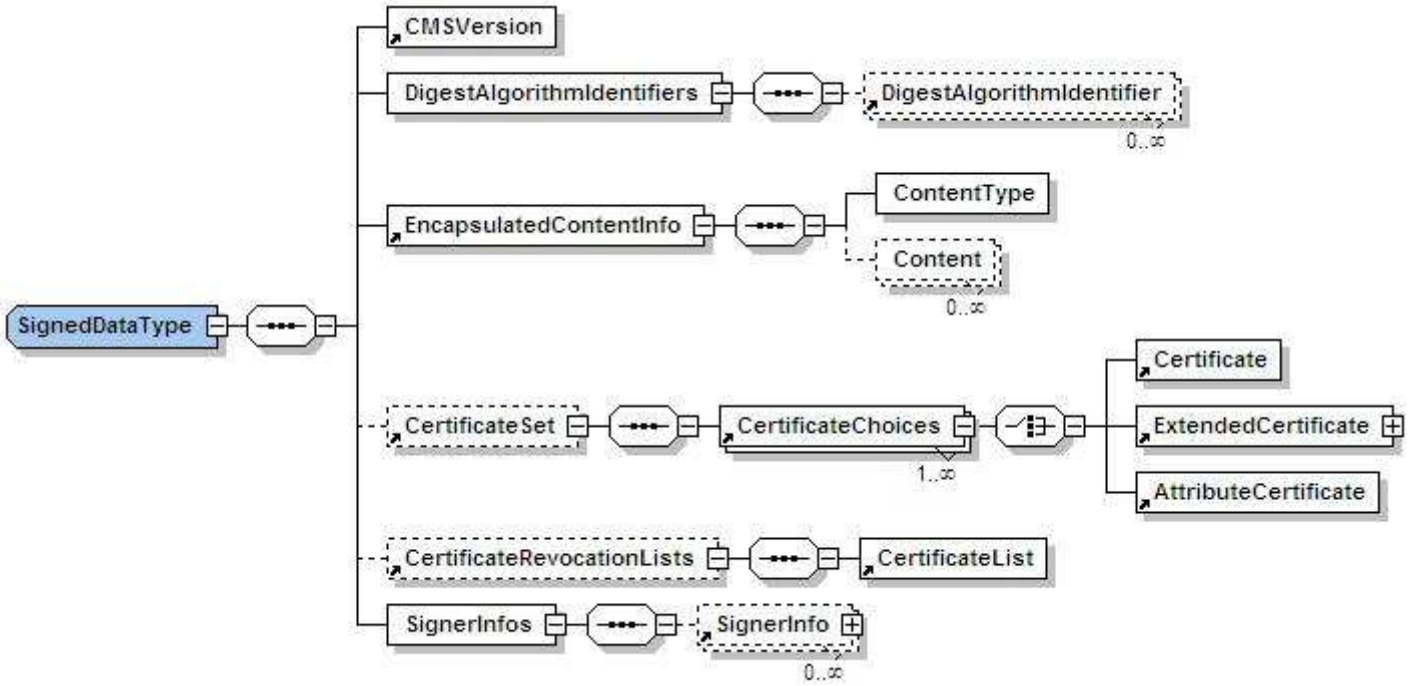


RFC 3280

Certificados X.509

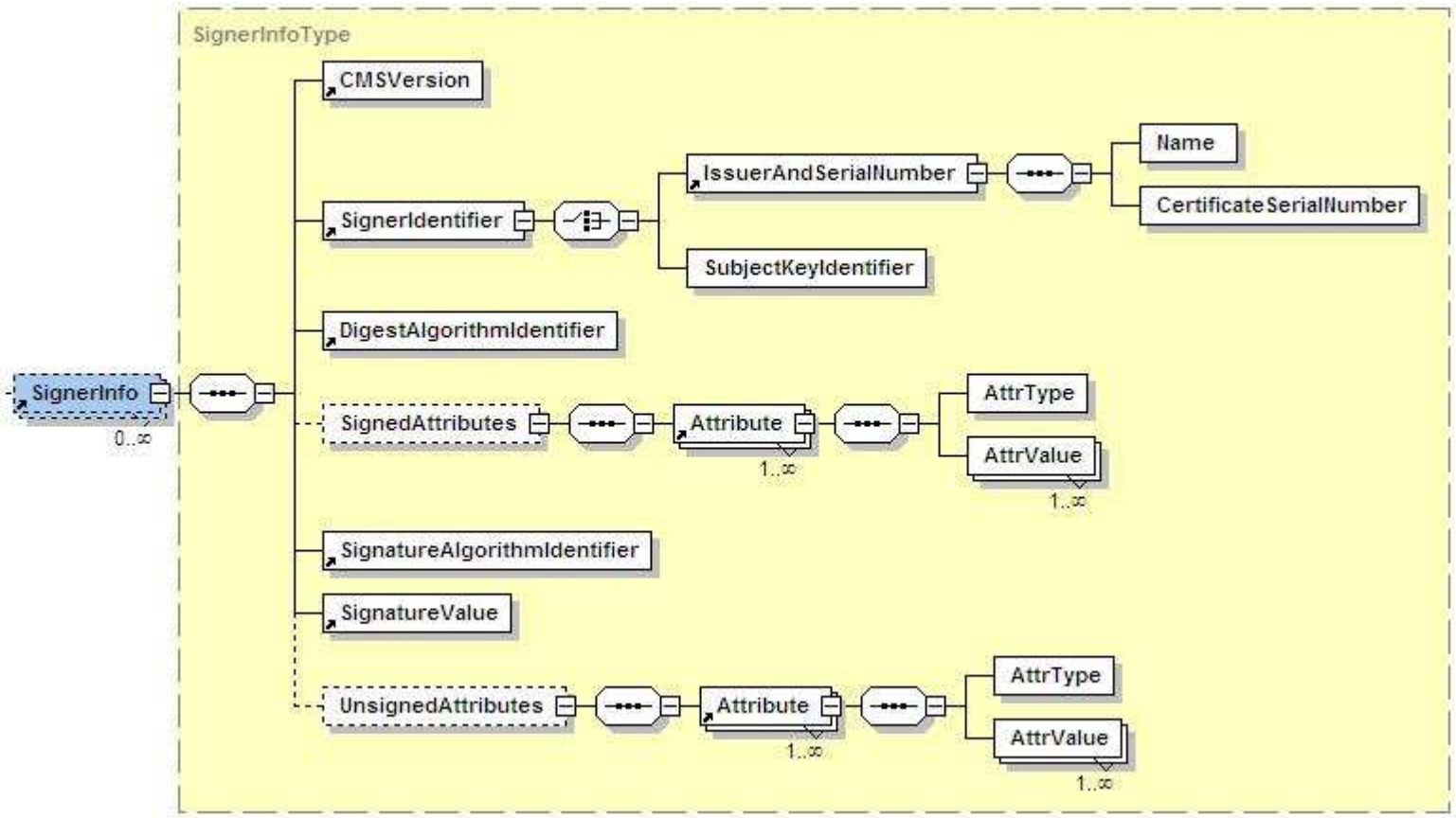


Formato de Firma (CMS - SignedData)



RFC 3852 – Versión
IETF de PKCS#7

Formato de Firma (CMS - SignedData)



OpenSSL

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

Implementación Open Source de diversos algoritmos y estándares criptográficos. http://www.openssl.org

Documentación de uso:

http://www.madboa.com/geek/openssl/

Side Channel

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA

- Definición: Es un tipo de ataque basado en información obtenida (de un efecto secundario) de la implementación del algoritmo criptográfico y no basada en debilidades del algoritmo en sí.

- Tipos de Side Channels:
  - Tiempo: basados en cuánto tardan ciertos cómputos.
  - Consumo eléctrico: basados en diferencias de consumo del hardware dependiendo de la operación realizada.
  - Electromagnéticos: basados en información fugada como radiación electromagnética.
  - Acústico: basados en sonidos emitidos durante el cómputo.
  - etc.

Forward Secrecy

- **Dependiendo de como se genera e intercambia la clave de sesión, en, por ejemplo, ssl, el que obtenga la clave privada del servidor, podría descifrar todas las comunicaciones previas.**

- **Para evitar eso se usa Forward Secrecy.**

- **Ref: https://community.qualys.com/blogs/securitylabs/2013/06/25/ssl-labs-deploying-forward-secrecy**

Padding Oracle Attacks

- Escenario: Una aplicación que utiliza un cifrador de bloques en modo CBC y padding PKCS#5. La aplicación responde de la siguiente manera:
  - Texto valido correctamente cifrado: respuesta normal.
  - Texto inválido correctamente cifrado: error indicando que el valor recibido no es válido.
  - Texto con cifrado incorrecto (padding incorrecto): error indicando falla de padding.

- En este escenario el ataque nos permite descifrar el mensaje y cifrar un mensaje arbitrario (sin conocer la clave simétrica).

- Ref: http://netifera.com/research/poet/PaddingOracleBHEU10.pdf

Otras aplicaciones de criptografía

- **Mental Poker**
- **Zero-knowledge proofs**
- **Simultaneous Contract Signing**
- **Secure elections**
- **Digital Cash**

Más bibliografía

DEPARTAMENTO DE COMPUTACION
Facultad de Ciencias Exactas y Naturales - UBA