MTAT.07.017
Applied Cryptography

Rakenduslik krüptograafia
Прикладная криптография

Juri Hudolejev
University of Tartu
Spring 2011

Topic for This Week

Cryptographic Message Syntax (CMS)

BouncyCastle library for S/MIME and CMS

`org.bouncycastle.cms.*`

`org.bouncycastle.asn1.cms.*`

Hybrid Encryption

```
enc1 = encrypt(msg, K)
enc2 = encrypt(K, K+)
 → → → → enc1, enc2  → → → →
        //decrypt enc2 and enc1
```

Problem: how to get K+?

Problem: how to serialize **enc1** and **enc2**?

Cryptographic Message Syntax

Describes container for various cryptographic messages: signed data, encrypted data etc.

6 content types described in RFC 5652

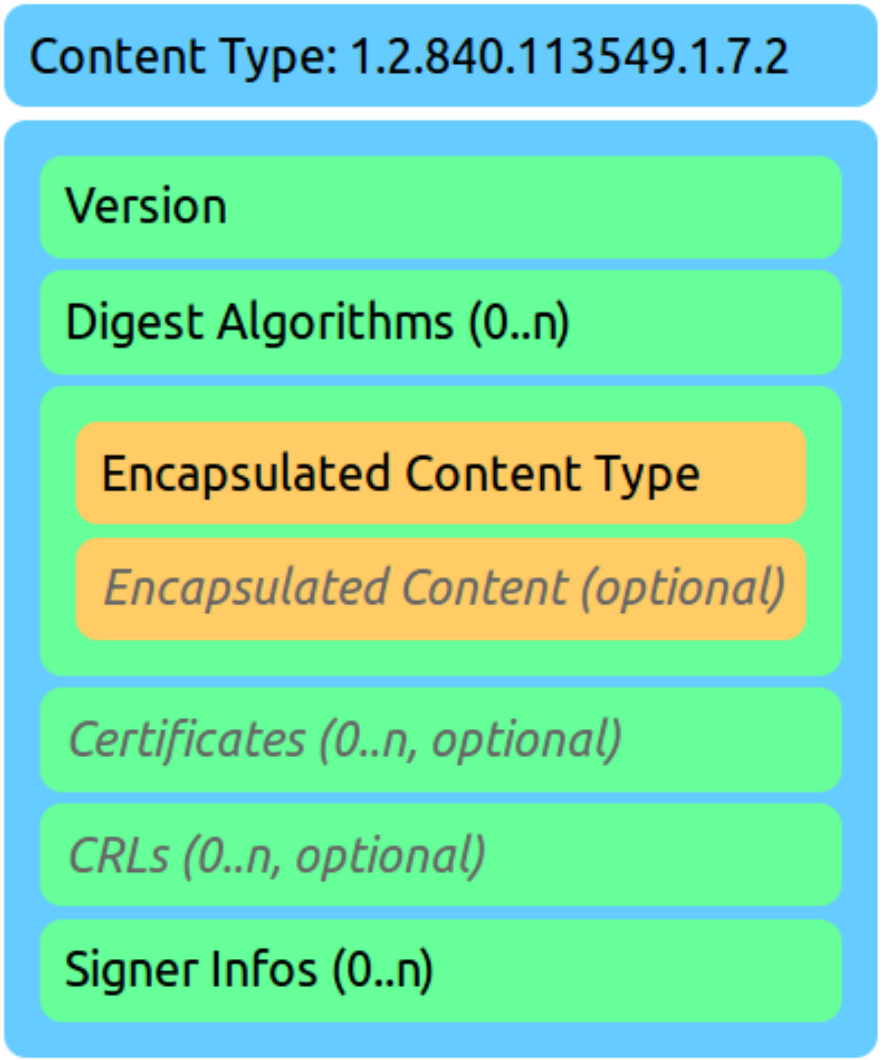
http://tools.ietf.org/html/rfc5652

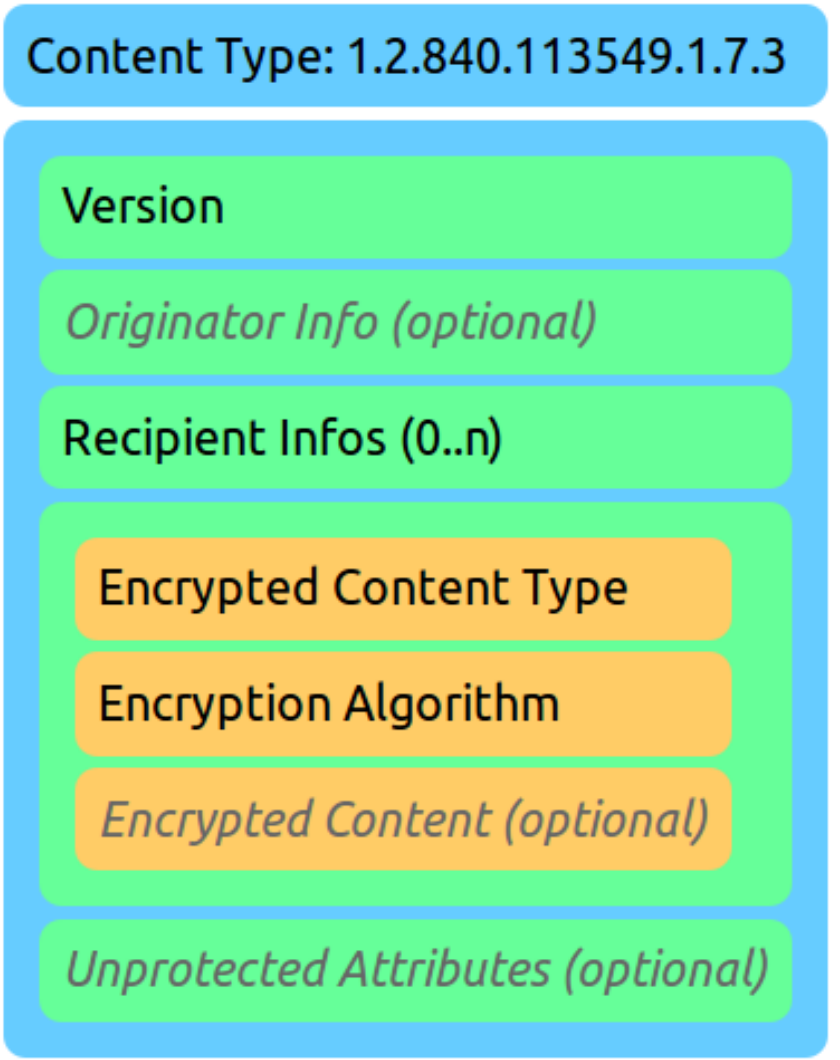
CMS Internals: `ContentInfo`

```
ContentInfo ::= SEQUENCE {
   conetntType  OBJECT IDENTIFIER,
   content   [0] EXPLICIT ANY
                 DEFINED BY contentType
}
```

RFC: http://tools.ietf.org/html/rfc5652#section-3

CMS Examples





CMS Type `signedData`

Signed message + signatures

```
ContentInfo ::= SEQUENCE {
   conetntType   OBJECT IDENTIFIER,
   content       [0] EXPLICIT SignedData
}
```

OID: http://www.oid-info.com/get/1.2.840.113549.1.7.2

RFC: http://tools.ietf.org/html/rfc5652#section-5

CMS Type `envelopedData`

Encrypted message + encrypted key for every recipient

```
ContentInfo ::= SEQUENCE {
   conetntType   OBJECT IDENTIFIER,
   content       [0] EXPLICIT EnvelopedData
}
```

OID: http://www.oid-info.com/get/1.2.840.113549.1.7.3

RFC: http://tools.ietf.org/html/rfc5652#section-6

CMS Type `encryptedData`

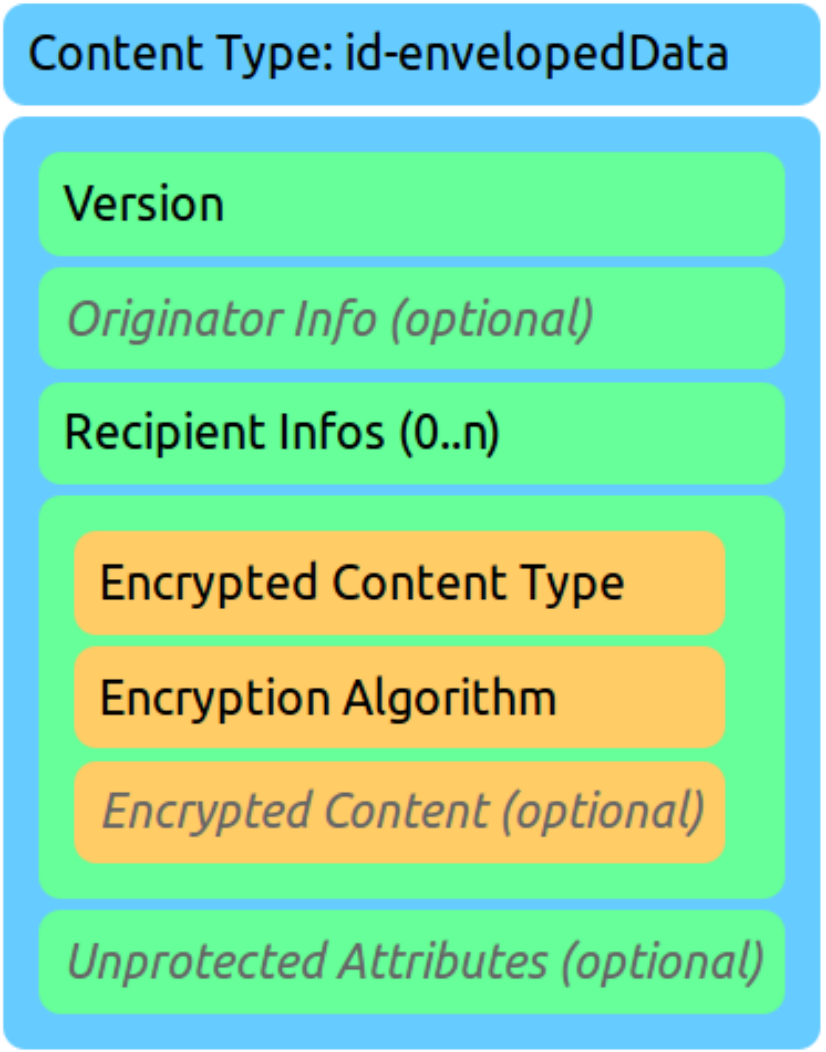
Encrypted message only – no keys nor recipients

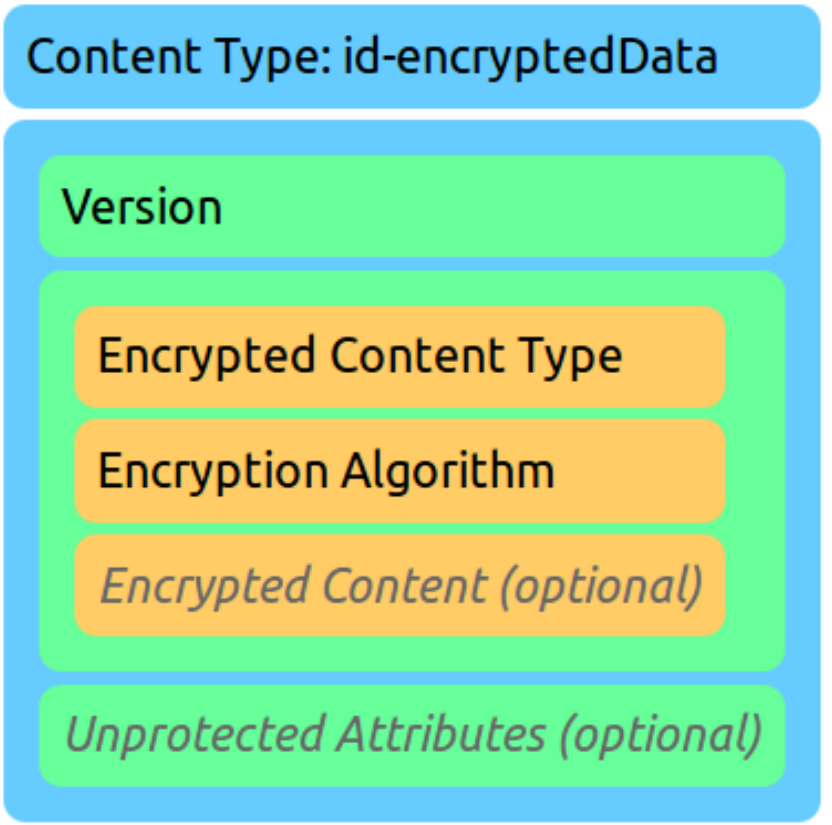
```
ContentInfo ::= SEQUENCE {
   conetntType   OBJECT IDENTIFIER,
   content       [0] EXPLICIT EncryptedData
}
```

OID: http://www.oid-info.com/get/1.2.840.113549.1.7.6

RFC: http://tools.ietf.org/html/rfc5652#section-8

Enveloped vs Encrypted Data





CMS Type `digestedData`

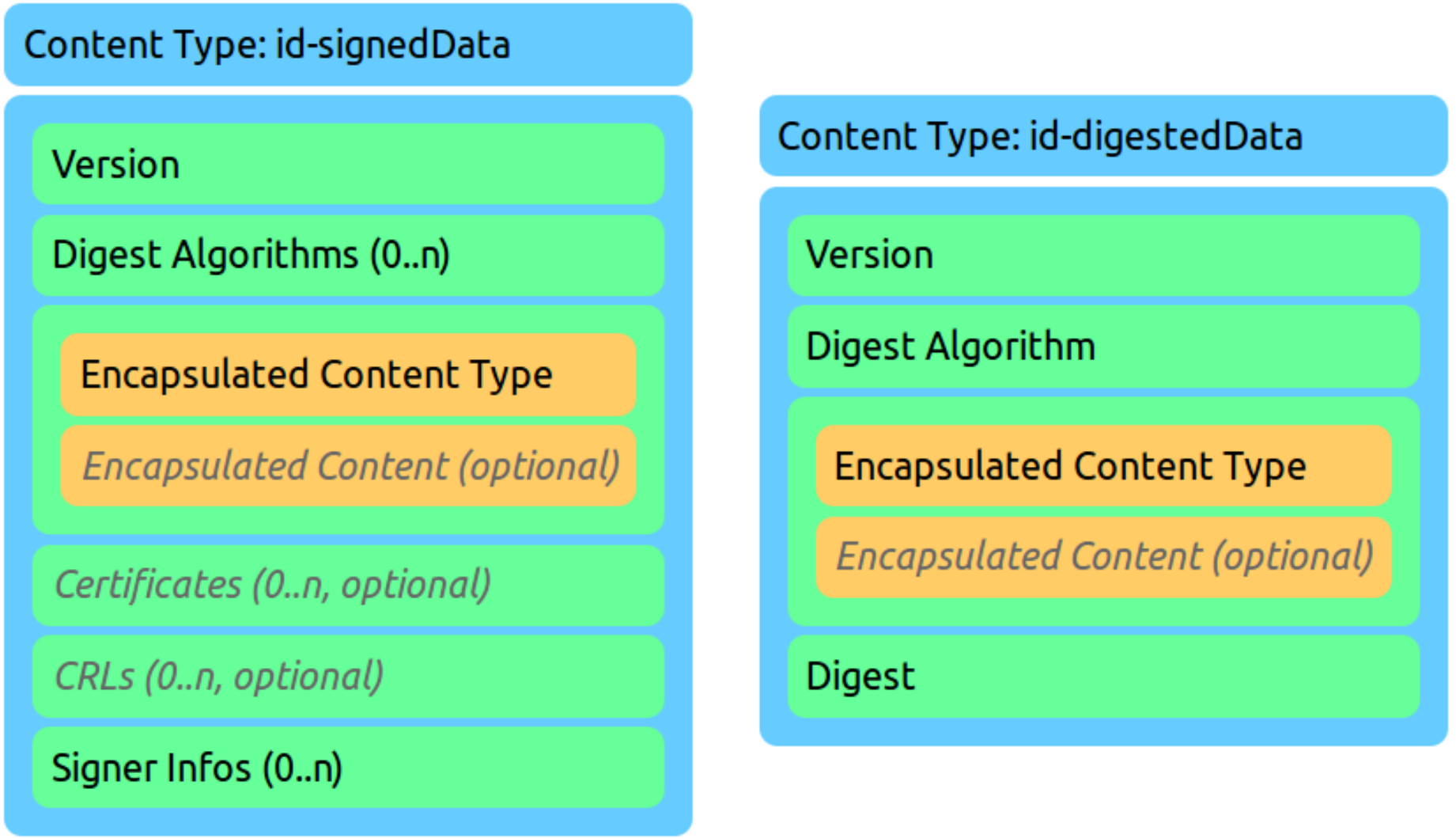
Message + message digest

```
ContentInfo ::= SEQUENCE {
   conetntType   OBJECT IDENTIFIER,
   content       [0] EXPLICIT DigestedData
}
```

OID: http://www.oid-info.com/get/1.2.840.113549.1.7.5

RFC: http://tools.ietf.org/html/rfc5652#section-7

Signed vs Digested Data



CMS Type `authenticatedData`

Message + MAC + authentication keys for every recipient

```
ContentInfo ::= SEQUENCE {
   conetntType   OBJECT IDENTIFIER,
   content   [0] EXPLICIT AuthenticatedData
}
```

http://www.oid-info.com/get/1.2.840.113549.1.9.16.1.2

RFC: http://tools.ietf.org/html/rfc5652#section-9

CMS Type `data`

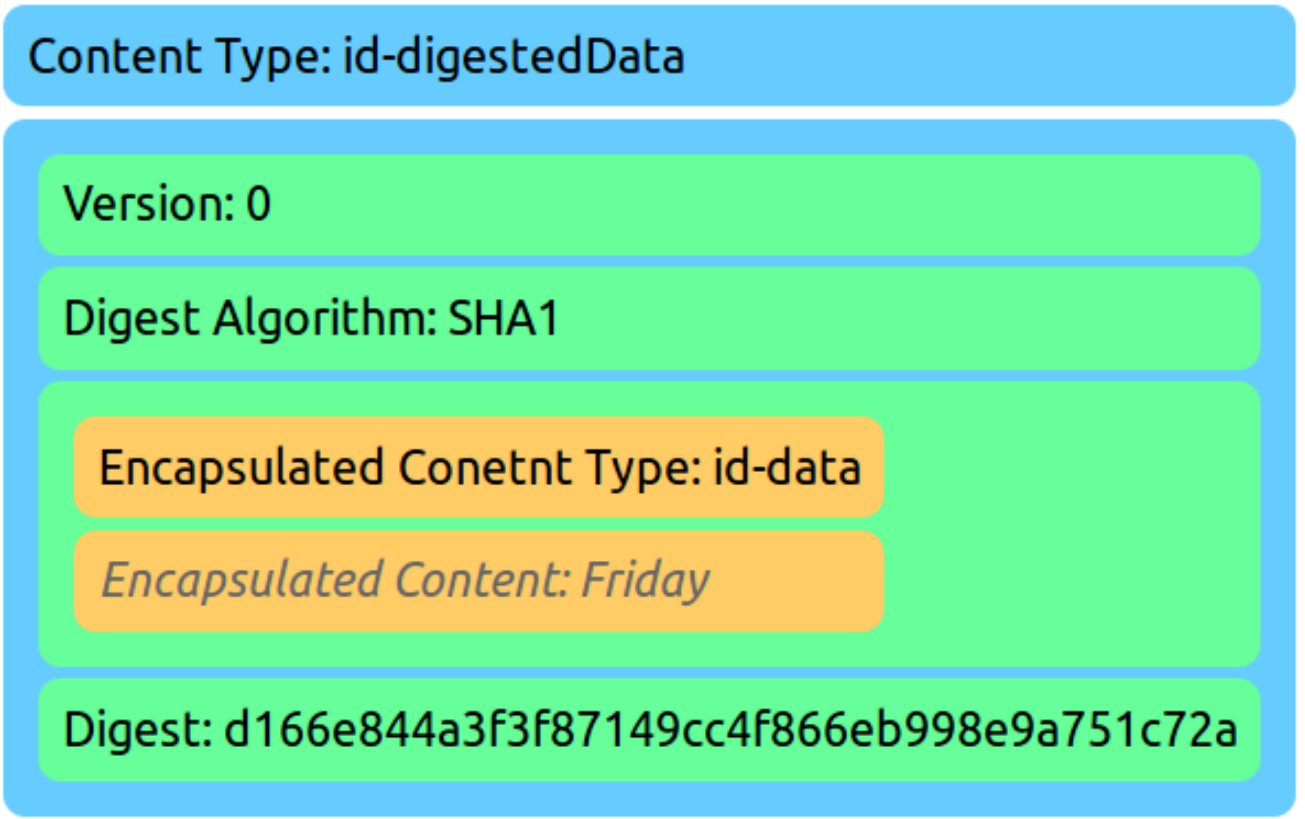
Raw data

```
ContentInfo ::= SEQUENCE {
   conetntType   OBJECT IDENTIFIER,
   content       [0] EXPLICIT OCTET STRING
}
```

OID: http://www.oid-info.com/get/1.2.840.113549.1.7.1

RFC: http://tools.ietf.org/html/rfc5652#section-4

CMS Type `data`



CMS Type `data`

`compressedData`

OID: 1.2.840.113549.1.9.16.1.9

RFC: http://tools.ietf.org/html/rfc3274

`timestampedData`

OID: 1.2.840.113549.1.9.16.1.31

RFC: http://tools.ietf.org/html/rfc5544

… and others

Questions?

EOF

Homework
http://courses.cs.ut.ee/2011/appcrypto/Main/Lab08

Deadline: Friday 2011-04-22 **08:00** EEST

Next lab session:

Friday 2011-04-15 **08:30** EEST @ Liivi 2 - 205