MTAT.07.017
Applied Cryptography

Rakenduslik krüptograafia
Прикладная криптография

Juri Hudolejev
University of Tartu
Spring 2011

Topic for This Week

Cryptographic timestamps

BouncyCastle library for timestamping

`org.bouncycastle.tsp.*`
`org.bouncycastle.asn1.tsp.*`

Timestamp?

SQL timestamp – type ('2011-04-15 09:03:01')

UNIX timestamp – value (1302858181)

ICMP timestamp – message for synchronization

Trusted timestamp – cryptography involved

Timestamp?

“Timestamp”

- Non-cryptographic context
- Many cryptographic timestamping implementations

“Time-stamp”, “TimeStamp”

- Most cryptographic standards and documents

“Time stamp”

Handwritten Signature

How to identify signer?

How to protect signature from forgery?

How long is signature valid?

How to repudiate the signature?

Digital Signature

Signing key is identified by certificate

To forge, copy of signing key is needed

Signature *may be* valid if certificate is verified

To repudiate, just declare certificate invalid

Certificate Status

Trust chain: can the certificate (issuer) be trusted?

OCSP: is the certificate valid **now**?

CRL: was the certificate valid **then**?

Problems:

- Certificates are removed from CRL when validity period ends
- Can we trust the time values in CRL?

Trusted Timestamp

Binds the state of data to time

Issued by trusted third party – TSA

Techniques described in RFC 3161

- Also in ANSI X9.95, ETSI TS 101 861, ISO/IEC 18014

Trusted Timestamp

Signed statement of timestamping authority:

```
> This data was presented to me
> at this time: [data] [time]
> ---
> Yours,
> TSA
> [signature]
```

Simplest Trusted Timestamp

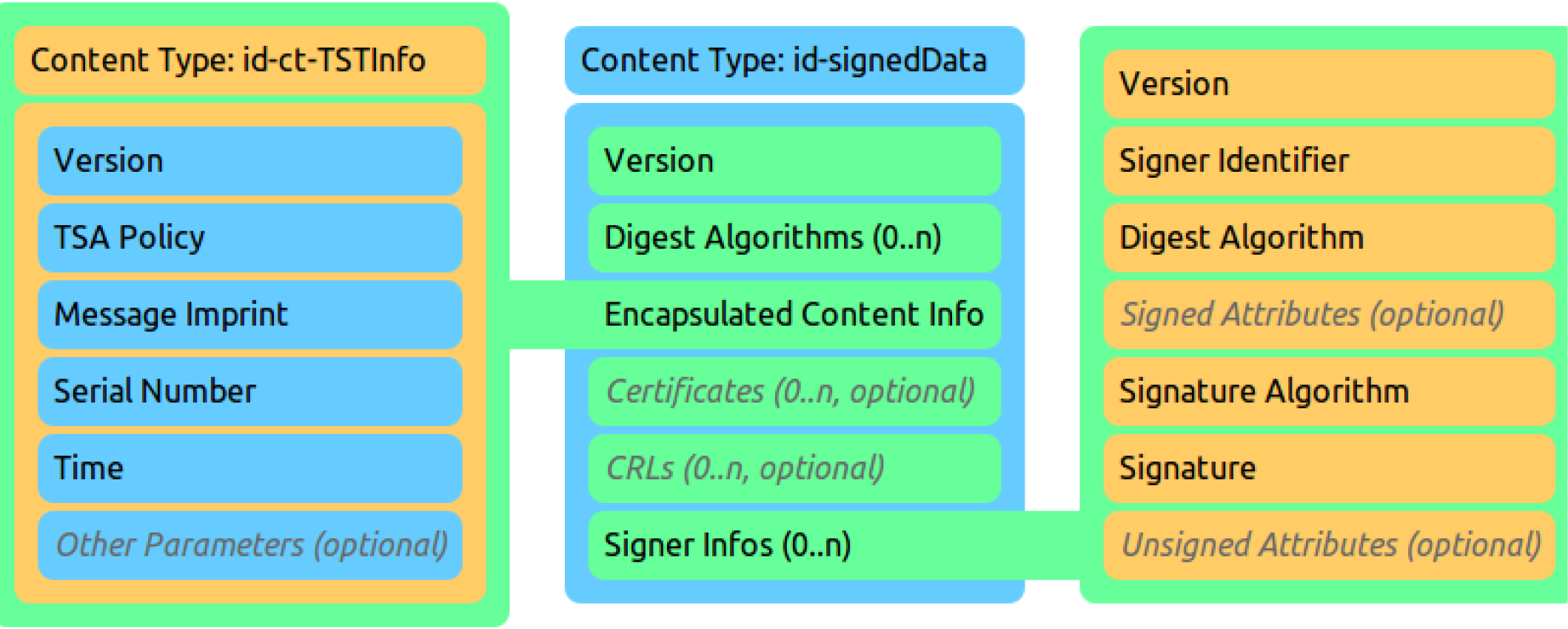
```
Timestamp ::= SEQUENCE {
    digest          OCTET STRING,
    time            GeneralizedTime,
    tsaSignature    Signature
}

Signature ::= ContentInfo
```

How Timestamping Works

```
dh = digest(msg)
req = tsReq(dh)
        → → → → → req → → → → →
                  ts = timestamp(req.dh)
                        resp = tsResp(ts)
        ← ← ← ← ← resp ← ← ← ← ←
ts = resp.ts
```

RFC 3161 Timestamp



Further Reading

Wikipedia: Trusted Timestamping

http://tools.ietf.org/html/rfc3161

http://globaltrustfinder.com/TSADefault.aspx

Questions?

\0

No extra homework for next week

Deadline to submit homeworks 7 and 8:

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

Next lab session:

Friday 2011-04-29 **08:30** EEST @ Liivi 2 - 205