

Security Record



Kevin Wilson
Greg Cannon
Jeff Stapleton
Anne Wang
Mike McCabe

BSI2000
Crossmatch
Innove
Cogent Systems
NIST

Why Security?



- Protect Document Integrity
- Connect Personal Data to Biometric Data
- Security at the Document Level
- Personal Responsibility

Words



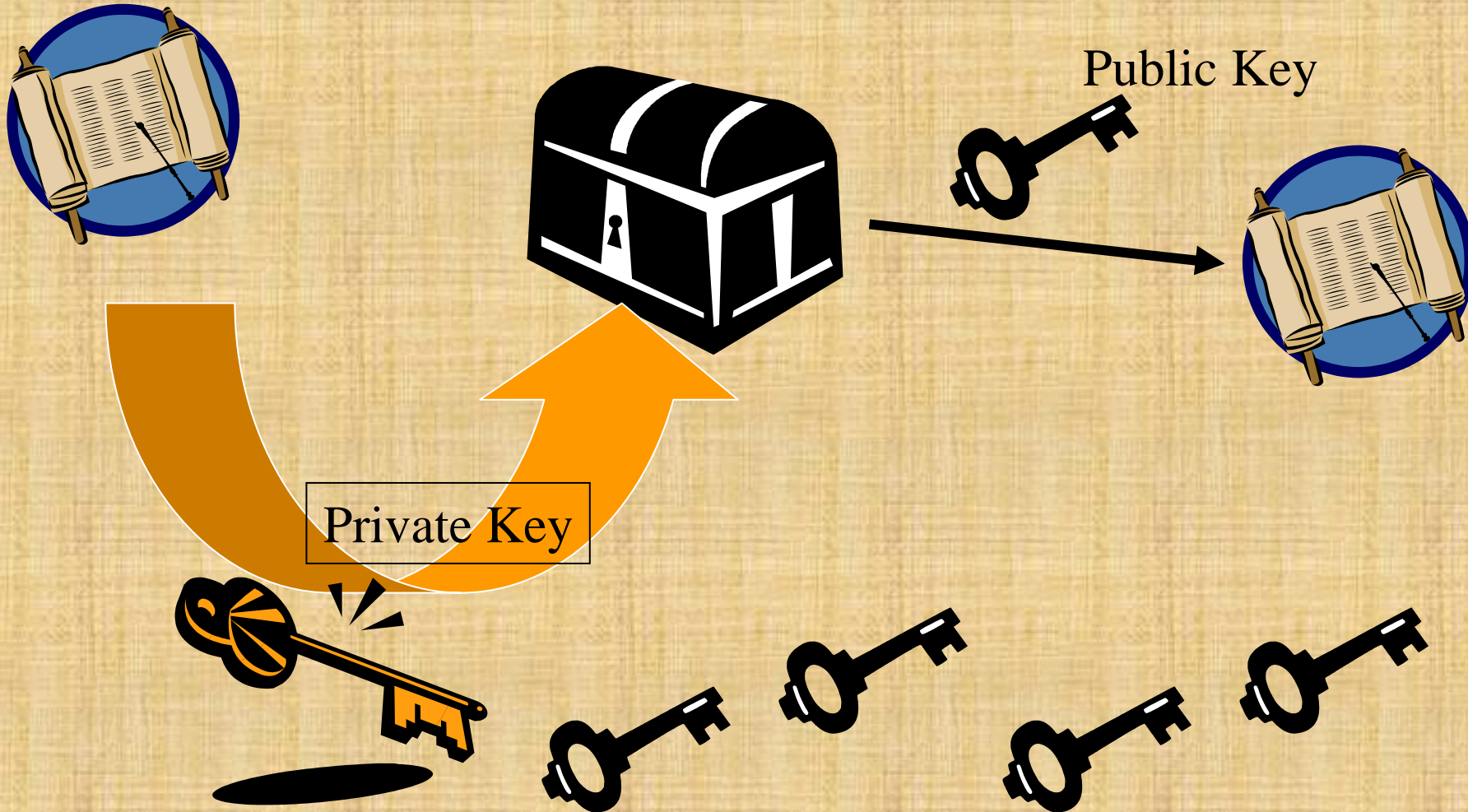
- Hash or Digest
- Digital Signature
 - ◆ Public/Private Key Cryptography
- Certificates
- Certificate Authorities
- Time Stamp Authorities

What is a Hash or Digest?



- Digested data
 - ◆ Small but reproducible
 - ◆ Fixed size for a given method
- Small changes in input lead to large changes in output
- Hard to make the same digest from different data
- One way

Public/Private Key Cryptography



Digital Signature



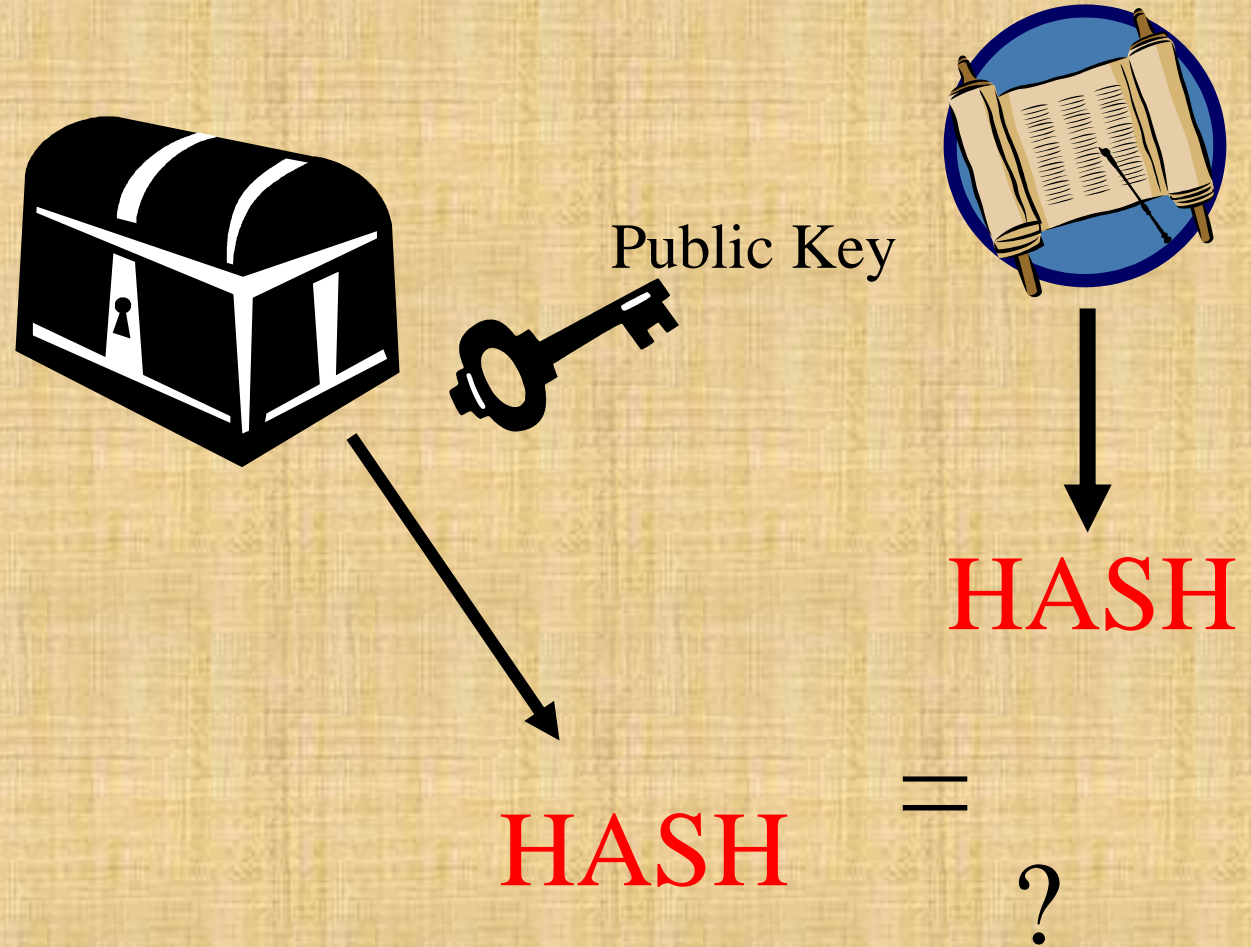
HASH



Private Key



Digital Signature

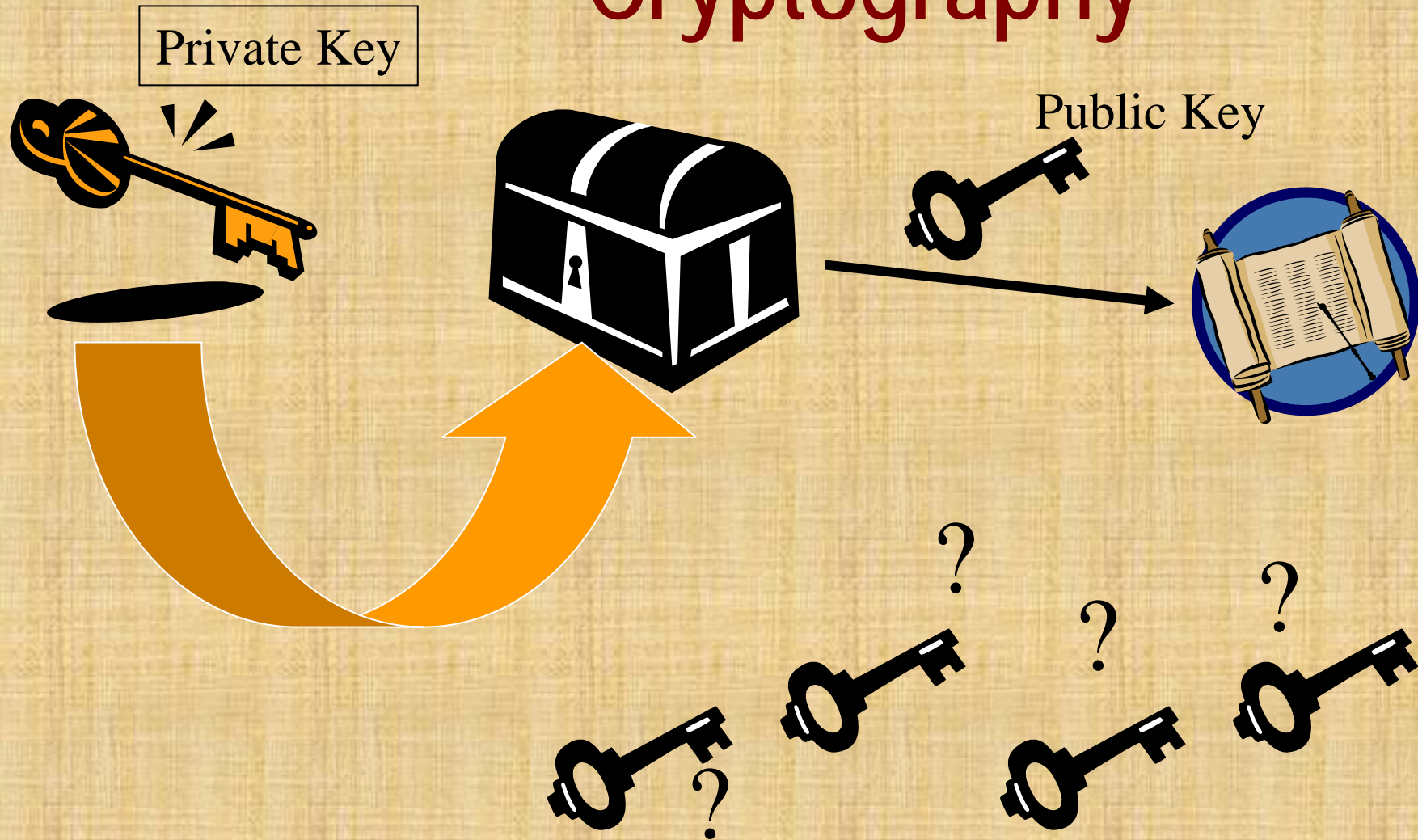


Digital Signature

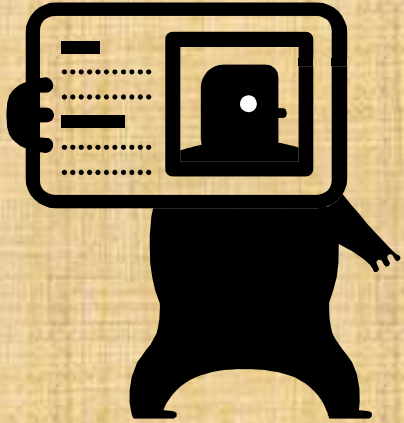


- Confidence that the signed data has not changed
- Non-repudiation

Public/Private Key Cryptography



Certificate Authority



Identity



Certificate

Time Stamp Authority



HASH



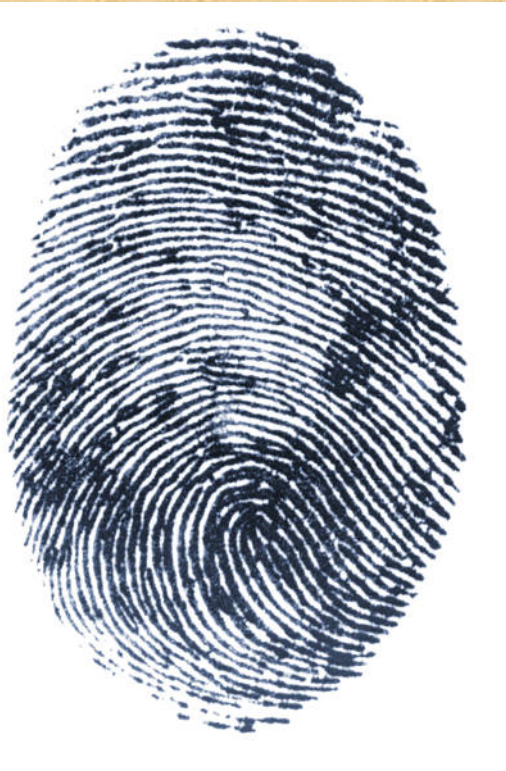
HASH

The Security Record



- New Record
 - ◆ Compatibility with earlier versions
- Optional
 - ◆ At the Document level
- Zero to Many
 - ◆ As document travels upstream

Security Record



- Set of Hashes
 - ◆ Linked to record by IDC and Type
- Signature over the Set of Hashes
- Algorithms as per policy
 - ◆ NIST SP 800-57
 - ◆ NIST SP 800-73

The Security Record



- Uses Cryptographic Message Syntax (CMS)
 - ◆ Also used in
 - ★ Secure email (S/MIME)
 - ★ SSL/TLS (https://)
 - ★ PIV Card
 - ◆ PKCS#7 since 1991 RSA
 - ◆ ASN.1 BER encoding

Hash of Each Record

APPLICANT		Doe, John, James		IDENT NAME	
NAME AND ADDRESS Billy Bob 1234 Main St Denver, CO 80202		PLACE BLUE Somewhere Ville		DATE OF BIRTH 03 16 1968	
CITY AND STATE US		SEX M		RACE W	
HEIGHT 5' 10"		WEIGHT 200		HAIR BRN	
EYES BRN		SCARS IL		MARKS	
FINGERPRINTS GA1111222		SOCIAL SECURITY NO. AF3334444		MILITARY SERVICE 353-22-4444	
Background Check					

HASH #####
HASH #####
HASH #####
HASH #####
HASH #####
HASH #####
HASH #####
HASH #####
HASH #####
HASH #####
HASH #####
HASH #####
HASH #####
HASH #####
HASH

Signature

Using Security with PKI



- Booking/Enrollment Officer
 - ◆ State or Local or National PKI
 - ◆ Upstream confidence
- Upstream Agents
 - ◆ Downstream confidence

Using Security without PKI



- Booking Officer
 - ◆ Self-Signed certificate
 - ★ Password or otherwise protected
- Upstream Agents
 - ◆ Self-signed certificates stamp as received/sent

Implementation



- CMS Signature
 - ◆ Microsoft CryptoApi
 - ◆ OpenSSL
 - ◆ Java
 - ◆ RSA, Certicom
 - ◆ PIV Card
- Certificate Authority
 - ◆ Microsoft Server CA
 - ◆ OpenSSL CA

PIV Enrollment and Infrastructure



Identity



Summary



- Strengthen Security by Embedding Security within the Document
- Straight forward to implement

Security Committee



- Greg Cannon
 - ◆ Crossmatch Technologies
- Michael McCabe
 - ◆ NIST
- Jeff Stapleton
 - ◆ Innove
- Anne Wang
 - ◆ Cogent Systems
- Kevin Wilson
 - ◆ BSI2000

Questions & Discussion



New Record



- 17.001:4 character length<gs>
- 17.002:IDC character<gs>
- Optional unsigned attributes
- 17.050:Signing OID<gs>
- 17.051:Signature or Timestamp<gs>
- 17.052:Digest OID<gs>
- Optional signed attributes
- 17.096:size of 17.050 through 17.096<gs>
- 17.097:character count of IDC to follow<gs>
- 17.098:IDC<us>hash<rs>IDC<us>hash<rs>...<gs>
- 17.099:CMS<gs>

	Type 19 Record
LENGTH (LEN)	19.001:0907<gs>
IMAGE DESIGNATION CHARACTER (IDC)	19.002:16<gs>
optional unsigned attributes	
SIGNING OID (SSO)	19.050:1.2.840.113549.7.2<gs>
CONTENT TYPE (SCT)	19.051:01<gs>
DIGEST OID (DGO)	19.052:1.3.14.3.2.26<gs>
optional signed attributes	
LENGTH OF SIGNED ATTR (LAS)	19.096:10<gs>
COUNT OF DIGESTS (CDI)	19.097:17<gs>
LIST OF DIGEST (LDI)	19.098:
	-1<us>01<us><20 binary bytes><rs>
	00<us>02<us><20 binary bytes><rs>
	01<us>04<us><20 binary bytes><rs>
	02<us>04<us><20 binary bytes><rs>
	03<us>04<us><20 binary bytes><rs>
	04<us>04<us><20 binary bytes><rs>
	05<us>04<us><20 binary bytes><rs>
	06<us>04<us><20 binary bytes><rs>
	07<us>04<us><20 binary bytes><rs>
	08<us>04<us><20 binary bytes><rs>
	09<us>04<us><20 binary bytes><rs>
	10<us>04<us><20 binary bytes><rs>
	11<us>04<us><20 binary bytes><rs>
	12<us>04<us><20 binary bytes><rs>
	13<us>04<us><20 binary bytes><rs>
	14<us>04<us><20 binary bytes><rs>
	15<us>04<us><20 binary bytes><gs>
CMS (SignedData) (AUT)	19.099:<335 binary bytes of DER encoded CMS>

Summary of Tables 2 and 3 From SP 800-57

Cryptographic Strength	Symmetric Algorithm	Hash Algorithm	ECC Algorithms	RSA/DSA/DH Algorithms
56-bits	DES	-	-	-
80-bits	3DES-2K	SHA-1 (160)	160-bits	1024-bits
112-bits	3DES-3K	SHA-2 (224)	224-bits	2048-bits
128-bits	AES-128	SHA-2 (256)	256-bits	3072-bits
192-bits	AES-192	SHA-2 (384)	384-bits	7680-bits
256-bits	AES-256	SHA-2 (512)	512-bits	15360-bits

ECC SignedData Example

Field	Value	Size
OID ₁	OID cms-ct-signed-data { 1 . 2 . 840 . 113549 . 1 . 7 . 2 }	9 bytes
Version ₂	Version number (1)	1 byte
OID ₃	OID fips-sha1 { 1 . 3 . 14 . 3 . 2 . 26 }	5 bytes
OID ₄	OID cms-ct-data { 1 . 2 . 840 . 113549 . 1 . 7 . 1 }	9 bytes
Detached Data ₅	File content is not encapsulated in the SignedData object	0 bytes
Version ₆	Version number (1)	1 byte
OID ₇	OID pkix-at-common-name { 2 . 5 . 4 . 3 }	3 bytes
Subject Name ₈	Issuer common name "Subject"	7 bytes
Serial Number ₉	Serial number hex "78 8C 29 19 99 25 FA 0B"	8 bytes
OID ₁₀	OID fips-sha1 { 1 . 2 . 14 . 3 . 2 . 26 }	5 bytes
OID ₁₁	OID ecdsa-with-sha1 { 1 . 2 . 840 . 10045 . 4 . 1 }	7 bytes
Signature ₁₂	ECDSA 328-bit digital signature from 163-bit ECC public key	41 bytes

References

- RFC3852 Cryptographic Message Syntax (July 2004, supersedes RFC3369, RFC2630, PKCS#7 1.5)
- NIST SP 800-57 Recommendation for Key Management (8/2005)
- ISO/IEC 8824:2001 (All parts) | ITU-T Recommendation X.680-series (2000), Information Technology - Abstract Syntax Notation One (ASN.1)
- [8825] ISO/IEC 8825-1:2001 | ITU-T Recommendation X.690 (2000), Information Technology - ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

References continued

- ANSI X9.95-2005 Trusted Time Stamp Management and Security

CMS Structure

```
ContentInfo ::= SEQUENCE {
  contentType    ContentType, ..... OID1
  content [0] EXPLICIT ANY DEFINED BY contentType }
  SignedData ::= SEQUENCE {
    version CMSVersion ..... Version2
    digestAlgorithms DigestAlgorithmIdentifiers,
      DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier
      DigestAlgorithmIdentifier ::= AlgorithmIdentifier
      AlgorithmIdentifier ::= SEQUENCE {
        algorithm    OBJECT IDENTIFIER, ..... OID3
        parameters  ANY DEFINED BY algorithm OPTIONAL }
    encapsContentInfo EncapsulatedContentInfo,
      EncapsulatedContentInfo ::= SEQUENCE {
        eContentType ContentType, ..... OID4
        eContent [0] EXPLICIT OCTET STRING OPTIONAL } ..... Detached Data5
    certificates [0] IMPLICIT CertificateSet OPTIONAL
      CertificateSet ::= SET OF CertificateChoices
      CertificateChoices ::= CHOICE {
        certificate Certificate,
        extendedCertificate [0] IMPLICIT ExtendedCertificate, -- Obsolete --
        v1AttrCert [1] IMPLICIT AttributeCertificateV1,      -- Obsolete --
        v2AttrCert [2] IMPLICIT AttributeCertificateV2,
        other [3] IMPLICIT OtherCertificateFormat }
    crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,
      RevocationInfoChoices ::= SET OF RevocationInfoChoice
      RevocationInfoChoice ::= CHOICE {
        crl CertificateList,
        other [1] IMPLICIT OtherRevocationInfoFormat }
    signerInfos SignerInfos
      SignerInfos ::= SET OF SignerInfo
      SignerInfo ::= SEQUENCE {
        version CMSVersion, ..... Version6
        sid SignerIdentifier,
```

```

signerInfos SignerInfos
  SignerInfos ::= SET OF SignerInfo
  SignerInfo ::= SEQUENCE {
    version CMSVersion, ..... Version6
    sid SignerIdentifier,
      SignerIdentifier ::= CHOICE {
        issuerAndSerialNumber IssuerAndSerialNumber,
          IssuerAndSerialNumber ::= SEQUENCE {
            issuer Name,
              type OBJECT IDENTIFIER ..... OID7
              value AttributeValue ..... Subject Name8
            serialNumber CertificateSerialNumber } ..... Serial Number9
        subjectKeyIdentifier [0] SubjectKeyIdentifier }
    digestAlgorithm DigestAlgorithmIdentifier,
      AlgorithmIdentifier ::= SEQUENCE {
        algorithm OBJECT IDENTIFIER,
        parameters ANY DEFINED BY algorithm OPTIONAL }
    signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL,
      SignedAttributes ::= SET SIZE (1..MAX) OF Attribute
      Attribute ::= SEQUENCE {
        attrType OBJECT IDENTIFIER, ..... OID10
        attrValues SET OF AttributeValue }
        AttributeValue ::= ANY
    signatureAlgorithm SignatureAlgorithmIdentifier,
      AlgorithmIdentifier ::= SEQUENCE {
        algorithm OBJECT IDENTIFIER, ..... OID11
        parameters ANY DEFINED BY algorithm OPTIONAL }
    signature SignatureValue,
      SignatureValue ::= OCTET STRING ..... Signature12
    unsignedAttrs [1] IMPLICIT UnsignedAttributes OPTIONAL
      UnsignedAttributes ::= SET SIZE (1..MAX) OF Attribute
      Attribute ::= SEQUENCE {
        attrType OBJECT IDENTIFIER,
        attrValues SET OF AttributeValue }
        AttributeValue ::= ANY
  } -- end of SignerInfo --
} -- end of SignedData --

```