Security Record

Kevin Wilson  BSI2000
Greg Cannon  Crossmatch
Jeff Stapleton  Innove
Anne Wang  Cogent Systems
Mike McCabe  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

Private Key
Public Key
Digital Signature

HASH

Private Key
Digital Signature

Public Key

HASH

HASH

=?
Digital Signature

- Confidence that the signed data has not changed
- Non-repudiation
Public/Private Key Cryptography

Private Key

Public Key
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

Signature

Hash of Each Record

# # # # # 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
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>
<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LENGTH (LEN)</td>
<td>19.001:0907.gs</td>
</tr>
<tr>
<td>IMAGE DESIGNATION CHARACTER (IDC)</td>
<td>19.002:16.gs</td>
</tr>
<tr>
<td>Optional unsigned attributes</td>
<td></td>
</tr>
<tr>
<td>SIGNING OID (SSO)</td>
<td>19.050:1.2.840.113549.7.2.gs</td>
</tr>
<tr>
<td>CONTENT TYPE (SCT)</td>
<td>19.051:01.gs</td>
</tr>
<tr>
<td>DIGEST OID (DGO)</td>
<td>19.052:1.3.143.2.26.gs</td>
</tr>
<tr>
<td>Optional signed attributes</td>
<td></td>
</tr>
<tr>
<td>LENGTH OF SIGNED ATTR (LAS)</td>
<td>19.096:10.gs</td>
</tr>
<tr>
<td>COUNT OF DIGESTS (CDI)</td>
<td>19.097:17.gs</td>
</tr>
<tr>
<td>LIST OF DIGEST (LDI)</td>
<td>19.098:</td>
</tr>
<tr>
<td></td>
<td>-1&lt;us&gt;01&lt;us&gt;&lt;20 binary bytes&gt;</td>
</tr>
<tr>
<td></td>
<td>00&lt;us&gt;02&lt;us&gt;&lt;20 binary bytes&gt;</td>
</tr>
<tr>
<td></td>
<td>01&lt;us&gt;04&lt;us&gt;&lt;20 binary bytes&gt;</td>
</tr>
<tr>
<td></td>
<td>02&lt;us&gt;04&lt;us&gt;&lt;20 binary bytes&gt;</td>
</tr>
<tr>
<td></td>
<td>03&lt;us&gt;04&lt;us&gt;&lt;20 binary bytes&gt;</td>
</tr>
<tr>
<td></td>
<td>04&lt;us&gt;04&lt;us&gt;&lt;20 binary bytes&gt;</td>
</tr>
<tr>
<td></td>
<td>05&lt;us&gt;04&lt;us&gt;&lt;20 binary bytes&gt;</td>
</tr>
<tr>
<td></td>
<td>06&lt;us&gt;04&lt;us&gt;&lt;20 binary bytes&gt;</td>
</tr>
<tr>
<td></td>
<td>07&lt;us&gt;04&lt;us&gt;&lt;20 binary bytes&gt;</td>
</tr>
<tr>
<td></td>
<td>08&lt;us&gt;04&lt;us&gt;&lt;20 binary bytes&gt;</td>
</tr>
<tr>
<td></td>
<td>09&lt;us&gt;04&lt;us&gt;&lt;20 binary bytes&gt;</td>
</tr>
<tr>
<td></td>
<td>10&lt;us&gt;04&lt;us&gt;&lt;20 binary bytes&gt;</td>
</tr>
<tr>
<td></td>
<td>11&lt;us&gt;04&lt;us&gt;&lt;20 binary bytes&gt;</td>
</tr>
<tr>
<td></td>
<td>12&lt;us&gt;04&lt;us&gt;&lt;20 binary bytes&gt;</td>
</tr>
<tr>
<td></td>
<td>13&lt;us&gt;04&lt;us&gt;&lt;20 binary bytes&gt;</td>
</tr>
<tr>
<td></td>
<td>14&lt;us&gt;04&lt;us&gt;&lt;20 binary bytes&gt;</td>
</tr>
<tr>
<td></td>
<td>15&lt;us&gt;04&lt;us&gt;&lt;20 binary bytes&gt;</td>
</tr>
<tr>
<td></td>
<td>19.099:&lt;335 binary bytes of DER encoded CMS&gt;</td>
</tr>
</tbody>
</table>
## Summary of Tables 2 and 3 From SP 800-57

<table>
<thead>
<tr>
<th>Cryptographic Strength</th>
<th>Symmetric Algorithm</th>
<th>Hash Algorithm</th>
<th>ECC Algorithms</th>
<th>RSA/DSA/DH Algorithms</th>
</tr>
</thead>
<tbody>
<tr>
<td>56-bits</td>
<td>DES</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>80-bits</td>
<td>3DES-2K</td>
<td>SHA-1 (160)</td>
<td>160-bits</td>
<td>1024-bits</td>
</tr>
<tr>
<td>112-bits</td>
<td>3DES-3K</td>
<td>SHA-2 (224)</td>
<td>224-bits</td>
<td>2048-bits</td>
</tr>
<tr>
<td>128-bits</td>
<td>AES-128</td>
<td>SHA-2 (256)</td>
<td>256-bits</td>
<td>3072-bits</td>
</tr>
<tr>
<td>192-bits</td>
<td>AES-192</td>
<td>SHA-2 (384)</td>
<td>384-bits</td>
<td>7680-bits</td>
</tr>
<tr>
<td>256-bits</td>
<td>AES-256</td>
<td>SHA-2 (512)</td>
<td>512-bits</td>
<td>15360-bits</td>
</tr>
</tbody>
</table>
**ECC SignedData Example**

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>OID&lt;sub&gt;1&lt;/sub&gt;</td>
<td>OID cms-ct-signed-data { 1.2.840.113549.1.7.2 }</td>
<td>9 bytes</td>
</tr>
<tr>
<td>Version&lt;sub&gt;2&lt;/sub&gt;</td>
<td>Version number (1)</td>
<td>1 byte</td>
</tr>
<tr>
<td>OID&lt;sub&gt;3&lt;/sub&gt;</td>
<td>OID fips-shal { 1.3.14.3.2.26 }</td>
<td>5 bytes</td>
</tr>
<tr>
<td>OID&lt;sub&gt;4&lt;/sub&gt;</td>
<td>OID cms-ct-data { 1.2.840.113549.1.7.1 }</td>
<td>9 bytes</td>
</tr>
<tr>
<td>Detached Data&lt;sub&gt;5&lt;/sub&gt;</td>
<td>File content is not encapsulated in the SignedData object</td>
<td>0 bytes</td>
</tr>
<tr>
<td>Version&lt;sub&gt;6&lt;/sub&gt;</td>
<td>Version number (1)</td>
<td>1 byte</td>
</tr>
<tr>
<td>OID&lt;sub&gt;7&lt;/sub&gt;</td>
<td>OID pkix-at-common-name { 2.5.4.3 }</td>
<td>3 bytes</td>
</tr>
<tr>
<td>Subject Name&lt;sub&gt;8&lt;/sub&gt;</td>
<td>Issuer common name “Subject”</td>
<td>7 bytes</td>
</tr>
<tr>
<td>Serial Number&lt;sub&gt;9&lt;/sub&gt;</td>
<td>Serial number hex “78 8C 29 19 99 25 FA 0B”</td>
<td>8 bytes</td>
</tr>
<tr>
<td>OID&lt;sub&gt;10&lt;/sub&gt;</td>
<td>OID fips-shal { 1.2.14.3.2.26 }</td>
<td>5 bytes</td>
</tr>
<tr>
<td>OID&lt;sub&gt;11&lt;/sub&gt;</td>
<td>OID ecdsa-with-shal { 1.2.840.10045.4.1 }</td>
<td>7 bytes</td>
</tr>
<tr>
<td>Signature&lt;sub&gt;12&lt;/sub&gt;</td>
<td>ECDSA 328-bit digital signature from 163-bit ECC public key</td>
<td>41 bytes</td>
</tr>
</tbody>
</table>
References

- RFC3852 Cryptographic Message Syntax (July 2004, supersedes RFC3369, RFC2630, PKCS#7 1.5)
- NIST SP 800-57 Recommendation for Key Management (8/2005)
References continued

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

ContentInfo ::= SEQUENCE {
  contentType Content-Type,.................. OID_1
  content [0] EXPLICIT ANY DEFINED BY contentType }
SignedData ::= SEQUENCE {
  version CMSVersion,.......................... Version_2
  digestAlgorithms Digest AlgorithmsIdentifiers,
    Digest AlgorithmsIdentifiers ::= SET OF Digest AlgorithmIdentifier
    Digest AlgorithmIdentifier ::= AlgorithmIdentifier
    AlgorithmIdentifier ::= SEQUENCE {
      algorithm OBJECT IDENTIFIER,.................. OID_3
      parameters ANY DEFINED BY algorithm OPTIONAL }
  encapsulatedContentInfo EncapsulatedContentInfo,
    EncapsulatedContentInfo ::= SEQUENCE {
      eContentType Content-Type,.................. OID_4
      eContent [0] EXPLICIT OCTET STRING OPTIONAL }................ Detached Data
  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,.......................... Version_5
    sid SignerIdentifier,
signerInfos  SignerInfos
   SignerInfos ::= SET OF SignerInfo
   SignerInfo ::= SEQUENCE {
      version CMSVersion, ................................................................. Version
      sid SignerIdentifier,
         SignerIdentifier ::= CHOICE {
            issuerAndSerialNumber IssuerAndSerialNumber,
               IssuerAndSerialNumber ::= SEQUENCE {
                  issuer Name,
                     type OBJECT IDENTIFIER.................................. OID
                  value AttributeValue................................. Subject Name
                  serialNumber CertificateSerialNumber } ........ Serial Number
            subjectKeyId SubjectKeyId } [0] SubjectKeyId
      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.......................... OID
               attrValues SET OF AttributeValue } 
            AttributeValue ::= ANY
      signatureAlgorithm SignatureAlgorithmIdentifier,
         AlgorithmIdentifier ::= SEQUENCE {
            algorithm OBJECT IDENTIFIER.......................... OID
            parameters ANY DEFINED BY algorithm OPTIONAL } 
      signature SignatureValue,
         SignatureValue ::= OCTET STRING.................................. Signature
      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 --