S/MIME Capabilities

Jim Schaad
Soaring Hawk Consulting

RSA Public Keys

- Same structure for RSA v1.5, PSS, OAEP

```
RSAKeyCapabilities ::= SEQUENCE {
    minKeySize        RSAKeySize,
    maxKeySize        RSAKeySize OPTIONAL
}
```

Elliptical Curve Keys

- Used for all elliptical curve keys

```
ECParameters ::= CHOICE {
  namedCurve      CURVE.&id({NamedCurve})
  -- implicitCurve   NULL
    -- implicitCurve MUST NOT be used in PKIX
  -- specifiedCurve  SpecifiedCurve
    -- specifiedCurve MUST NOT be used in PKIX
    -- Details for specifiedCurve can be found in [X9.62]
}
```

Diffie-Hellman Keys

- Used for DSA and DH

```
DSAKeyCapabilities ::= CHOICE {
        keySizes        [0] SEQUENCE {
          minKeySize            DSAKeySize,
          maxKeySize            DSAKeySize OPTIONAL
        },
        keyParams       [1] DSA-Params  (i.e. P, Q, G)
      }
```

RSASSA-PSS Signature

- No explicit hash algorithm

```
RsaSsa-Pss-sig-caps ::= SEQUENCE {
    hashAlg  SMIMECapability{{ HashAlgorithms }},
    maskAlg  SMIMECapability{{ MaskAlgorithmSet }}
                                    OPTIONAL,
    trailerField INTEGER DEFAULT 1
  }
```

Open Issue

- OCSP Algorithm Agility Document
  - Now in RFC Editor Queue
  - Uses AlgorithmIdentifier not S/MIME Capability for signature algorithm identifier
  - Options:
    - Fix in OCSP update document
    - Pull back and fix agility document
    - Don’t worry about it