Additional Algorithms and Identifiers for use of ECC with PKIX <pkix-ecc-pkalgs-03>

ID Author: Daniel R. L. Brown

Presented by: Brian Minard

Section 2.1

- Hash functions
- Extensible set based on SHA-1 and SHA-2 family
- Optional NULL parameters (is this needed?)

Section 2.2

- Key Derivation Functions
- To be updated
- Different choice of hash per KDF
- NIST SP 800-56A has a couple KDFs
- ANSI X9.63-2001 has a couple KDFs (to be updated with new SHA-2 family)

Section 2.4

- Message authentication codes
- Extensible list
- HMAC with SHA-xyz
- Parameter for truncating output
- Additional MACs?
- CMAC (NIST SP 800-38C)
- UMAC (RFC 4418)

Section 3

- Elliptic curve domain parameters
- Named curves: 15 NIST curves
- Specified curves:
- New feature:
- Hash used to generate curve
- E.g. SHA-256
- Base point G can be verifiably random

Section 4: ECC Algorithm Identifiers

- Usage Type 1, examples
- In SMIME protected email,
- Alice puts an ECC alg id
- Indicates what alg she used to protect message
- Cert sig field say what alg CA signed cert with
- Associate to issuer in cert

Section 4: ECC Algorithm Identifiers

- Usage type 2
- Placed into certificate
- Associated to subject
- Says what ECC algs the ECC key is to be used with
- Optional usage

Missing Syntax

- PKIX needs format for CA signatures
- How to encode ECDSA signature?
- Already defined in RFC 3279
- Makes sense to restate here

More Missing Syntax

- ECDH and ECMQV exchanges
- Public keys exchange
- Key confirmation messages (optional)
- Protocols can specify own formats (e.g. SMIME, SSH, TLS, IKE)
- PKIX may need for Proof of Possession?

Questions?