ASN.1 Module Revisions

Paul Hoffman

Jim Schaad

What Objects Do

- Associate Data and Types together
- Not part of the on the wire protocol

What Object Sets Do

- Collect a group of objects
- Allow filtering and searching
- Allow runtime modification
- API is not standard

Current State

- ALGORITHM
  - Pairs an OID and a type
  - Leads to lots of little objects
  - Type not optional
- Consider all items for Signature
- Omits implicit information in OID name

Proposal

Different Types for each Algorithm

- Digest
- Signature
- Asymmetric Key
- Key Transport
- Key Agreement
- Key Derivation
- Key Wrapping
- Bulk Encryption
- MAC
- (Missing items)

Signature Examples

DSA w/ SHA1

sig-DSA-sha1 SIGNATURE-ALGORITHM ::= {

IDENTIFIER id-dsa-with-sha1

PARAMS Dss-Sig-Value

ARE required

HASHS { hash-sha1 }

PUBLIC KEYS { pk-dsa }

}

RSA-PSS

sig-RSA-PSS SIGNATURE-ALGORITHM ::= {

IDENTIFIER id-RSASSA-PSS

PARAMS RSASSA-PSS-params

ARE required

HASH SET {hash-sha1 | hash-sha256, …}

PUBLIC KEY SET {pk-rsa | pk-rsa-pss }

}

Details

- Start of all items the same

  &id OBJECT IDENTIFIER UNIQUE,

  &ParamsType OPTIONAL,

  &paramsRequred ParamOptions DEFAULT required,

  &ValueType OPTIONAL

- Followed by fields specific to the algorithm type

Create & Use

- Define a known prefix for each object type
  - i.e. dig-, sig-, pk-,
- Decide how important automatic use is.
  - Different definitions of SIGNED in our rfc3280bis module

WE WANT FEEDBACK