Alternate Representations of the Public Key Cryptography Standards (PKCS) Using S-Expressions, S-PKCS

Matthew Wood Carl Ellison

Intel Corporation

1999 PKCS Workshop, Stockholm, Sweden

Why Define Data Encodings?

- Cross-platform data exchange
- Persistent storage
- Interoperability of independently implemented modules

Drawbacks of ASN.1 and BER/DER

- ✔ BER often includes several different, but equally valid encodings of the same data.
- ✔ Identity of data structures is assumed based on the context where it is found...
  - – within other data structures
  - – position within a higher level structure
- ✔ Parsing engine is large and complicated

Benefits of S-expressions

- ✔ Single encoding for any value
- ✔ Identity of all data structures is explicit
- ✔ Small, simple parsing engine
- ✔ Encoded structures are often shorter than their DER encoded versions

Examples: PKCS #1

- <digest-info>

  ```
  (sha1 #F47D…#)
  ```

- <rsa-public-key>

  ```
  (public-key
          (rsa
          (n #…#)
          (e #010001#)
          )
  )
  ```

Examples: PKCS #5

- <pbes2-params>

```
(pbes2-params
            (pkcs5-pbkdf2
            (pbkdf2-params
            (specified #...#)
            #03E8#
            (hmac-sha1)
            )
            )
            (des-cbc
            (iv #0123456789ABCDEF#)
            )
)
```

Questions?