PKCS Documents and ASN.1

Magnus Nystrom
RSA Laboratories
PKCS Workshop, 1999

RSA LABORATORIES

Background

- ASN.1 has been used in PKCS documents since the early days
- Only lately have truly compilable modules been included (PKCS #5 v2.0, PKCS #12 v1.0, PKCS #15v1.0)
- ASN.1 Syntax is varying between 1988 version and 1994 version in other documents (and is sometimes not even correct)

RSA LABORATORIES

Motivation

- This has led to some confusion (e.g. IMPLICIT or EXPLICIT tags?) and difficulties for developers
- Goals of the initiative presented here:
  - Make life easier for developers (enables use of ASN.1 compilers, conformance testing)
  - Simplify creation of test-vectors

RSA LABORATORIES

The Proposal

- **RSA Laboratories intends to publish *compilable* ASN.1 modules for all *active* PKCS documents that use ASN.1 (I.e. #1, #5, #7(?), #8, #9, #10, #12, #13, #15)**
- **These modules will cross-reference each other and import types from other standards as needed**

RSA LABORATORIES

The Proposal, II

- All modules will be written in the 1994/1997 ASN.1 notation (but will be compatible with existing documents using 1988 version)
- All modules will be published at RSA Laboratories' web site

RSA LABORATORIES

Other Modules

- With permission from ISO/IEC, we intend to publish ASN.1 modules from selected ISO standards as well, in order to simplify the task of compiling PKCS modules
- This will mostly be a subset of X.500 modules
- Same discussion with ANSI X9F1

RSA LABORATORIES

Time Plan

- Compilable ASN.1 modules for PKCS documents will be published during this fall
- Publication of selected (parts of) ISO/IEC and/or ANSI X9F1 modules will take place as soon as we receive permission to do so

RSA LABORATORIES

Contacting Us

- **Comments? Suggestions?**
  - **pkcs-tng@rsasecurity.com**
  - **pkcs-editor@rsasecurity.com**

RSA LABORATORIES