

PKCS: The Next Generation With a Progress Report on PKCS #11 (Cryptoki)

**Ray Sidney
RSA Laboratories**

1997 RSA Data Security Conference



PKCS: Public-Key Cryptography Standards

- Inter-vendor standards
- Actually more than just standards for public-key cryptography
- In extremely widespread use
- As compatible as possible with other standards, such as PEM and X.509



Current PKCS Documents

#1: RSA Encryption Standard

- Encryption
- Digital Signatures

#3: Diffie-Hellman Key-Agreement Standard

#5: Password-Based Encryption Standard

- MD2
- MD5
- DES



Current PKCS Documents (cont'd)

#6: Extended-Certificate Syntax Standard

#7: Cryptographic Message Syntax Standard

- Digital signatures
- Digital envelopes and encrypted data
- Hashed data

#8: Private-Key Information Syntax Standard

#9: Selected Attribute Types



Current PKCS Documents (cont'd)

#10: Certification Request Syntax Standard

**#11: Cryptographic Token Interface Standard
(Cryptoki)**



Events since the genesis of PKCS

- New cryptographic algorithms
- “Provably secure” ways of using RSA
 - OAEP
 - PSS
- P1363
- SET
- SDSI, SPKI
- 56 bits doesn’t seem so secure
- Problems with MD5



PKCS: The Next Generation

- **Currently soliciting suggestions**
 - Updates to existing PKCS documents
 - New PKCS documents
- **Hold workshop(s) in 1997**
- **Publish final specs in 1997-1998**



PKCS #1: RSA Encryption Standard

- Add in P1363 support
 - Encryption
 - Digital signatures
 - Elliptic curve/discrete logarithm methods



PKCS #3: Diffie-Hellman Key-Agreement Standard

- Add in P1363 support
 - Elliptic curve methods



PKCS #5: Password-Based Encryption Standard

- Additional hashing algorithms
 - SHA-1
- Support more encryption algorithms
 - Triple-DES
 - RC5



PKCS #6: Extended-Certificate Syntax Standard

- Superseded by the new version of X.509



PKCS #7: Cryptographic Message Syntax Standard

- Add in P1363 support
 - Encryption
 - Digital signatures
 - Elliptic curve methods/discrete logarithm methods
- Support for collecting several pieces of content together into an aggregate
- Support for attributes associated with a signed message (at present, all attributes are associated with a specific signer)



PKCS #8: Private-Key Information Syntax Standard

PKCS #9: Selected Attribute Types

- Looking good



PKCS #10: Certification Request Syntax Standard

- Certified Diffie-Hellman values



PKCS #11: Cryptographic Token Interface Standard (Cryptoki)

- **Cryptographic token**
 - Dedicated device for performing cryptographic functions
 - Hardware
 - Software
 - Can store objects
 - Tokens are inserted into slots for access
 - Access to sensitive information/capabilities is controlled by PIN



PKCS #11: Cryptoki (cont'd)

■ Cryptoki

- Application-level interface for using a token
- Supports multiple tokens and token types
- Supports multiple applications
- Very general



Cryptoki functions

- General purpose
- Slot and token management
- Session management
- Object management
- Encryption/decryption
- Message digesting
- Signing/MACing
- Verifying signatures/MACs
- Key management
- Random number generation
- Function management



History and future of Cryptoki

- **Announced in January 1994**
- **Workshop May 19-20, 1994**
- **v1.0 released April 28, 1995**
- **Workshop July 9-10, 1996**
- **v1.1 final spec**
- **v2.0**



Mechanisms in Cryptoki v1.0

- RSA encryption and signatures (several types)
- DSA
- Diffie-Hellman key exchange
- RC2 (ECB, CBC, MAC)
- RC4
- DES (ECB, CBC, MAC)
- Triple-DES (ECB, CBC, MAC)
- MD2
- MD5
- SHA-1



New mechanisms for Cryptoki

v1.1

- SSL/SPKM key derivation
- RC5
- CAST
- CAST3
- CAST5
- Fortezza support
- SET support
- Key wrapping with checksums
- Password-based encryption of data and keys
- Keyed hashing MACs, such as HMAC
- P1363 support
- Mechanisms combining digest and signature



Cryptoki v2.0

- Multi-user support
- Certificate-chain checking
- OIDs for specifying mechanisms
- Key escrow
- Token backup
- Timestamping
- Mechanisms and/or users as objects
- Token authenticity checks
- Token certification
- Security labels



PKCS #12: Personal Information Exchange Syntax Standard

- **Personal information associated with a user**
 - Certificates
 - Public and private keys
 - Miscellany



Conclusion

- Mailing list: `pkcs-tng@rsa.com`
 - Send email with “subscribe pkcs-tng” or “unsubscribe pkcs-tng” in message body to `majordomo@rsa.com`
- Mailing list: `cryptoki@rsa.com`
 - Send email with “subscribe cryptoki” or “unsubscribe cryptoki” in message body to `majordomo@rsa.com`
- PKCS editor: `pkcs-editor@rsa.com`

