PKCS Workshop ‘98
PKCS #12 / PFX Commentary

Blake Ramsdell

Chief (Applied) Cryptographer

Worldtalk Corporation

10/7/98

What am I yapping about

- Existing PKCS #12 complaints
  - Overly broad
  - Incompatible implementations (mostly resolved)
  - Multiple ways to do the same thing
  - Password-derived symmetric keys lumped in
  - No single source for information
  - “Am I doing this right?”

Limit the scope

- Define goals
  - Keep private keys secure
  - Use existing technology
  - Be precise
- Simplify!

Incompatible implementations

- What the spec said, what Vendor M did and what Vendor N did

Where do I put it?

- EncryptedPrivateKey vs. EncryptedData
- Heck, do both

Symmetric key derivation

- Belongs in PKCS #5, not lumped in with PKCS #12
- Stay within ASN.1 limitations
- Make sure there are no shortcuts for dictionary or other attacks

Finish the work

- We need a completed PKCS #12, not PKCS #12 plus email threads

Test vectors

- Uh, we need them

Contact information

Blake C. Ramsdell

<blaker@deming.com>
http://www.worldtalk.com