Some New RSA Mechanisms for PKCS #11

Burt Kaliski, RSA Laboratories

PKCS Workshop

April 14, 2003

Outline

- New mechanisms:
  - RSA-PSS
  - RSA-KEM
  - RSA-KEGVER
- Algorithm strategy
- Next steps

RSA-PSS

- Probabilistic Signature Scheme by Mihir Bellare, Phillip Rogaway
  - Adapted for standardization
- Security related to RSA problem in random oracle model
  - Higher assurance for the long term
- Supported in PKCS #1 v2.1, IEEE P1363a
- Recommended by NESSIE

RSA-PSS & PKCS #11

- RSA Laboratories encourages transition to RSA-PSS from PKCS #1 v1.5
  - Convenient as SHA-256+ deployed
- PKCS #11 already supports RSA-PSS, but not yet with SHA-256+
- **Recommendation:**
  - Add RSA-PSS/SHA-256+ in v2.20
  - Discourage PKCS #1 v1.5/SHA-256+

RSA-KEM

- Key Encapsulation Mechanism from Victor Shoup, *et al.*
- Security related to RSA problem in r.o. model
- Supported in draft ANS X9.44; proposed to TLS, S/MIME working groups
- Recommended by NESSIE

RSA-KEM Operations

- **Generate** key & corresponding ciphertext using public key (n,e)
  - R = random$[0,n\text{-}1]$
  - $C = R^e \bmod n$
  - K = KDF(R)
- **Regenerate** key from ciphertext using private key (n,d)
  - $R = C^d \bmod n$
  - K = KDF(R)

RSA-KEM for Key Wrapping

- **Wrap** keying material *KM* using (*n*,*e*):
  - (*C*, *KEK*) = Generate ((*n*,*e*))
  - *C*’ = Wrap (*KEK*, *KM*)
- Send (*C*,*C*’)
- **Unwrap** using (*n*,*d*):
  - *KEK* = Regenerate ((*n*,*d*), *C*)
  - *KM* = Unwrap (*KEK*, *C*’)

RSA-KEM & PKCS #11

- RSA Laboratories encourages transition to RSA-KEM from PKCS #1 v1.5
  - Convenient as AES deployed
- PKCS #11 doesn’t support RSA-KEM
- **Recommendation:**
  - Add RSA-KEM as PKCS #1 / TLS / S/MIME etc. updated

RSA-KEGVER

- Key generation with verifiable randomness by Ari Juels, Jorge Guajardo
- Key pairs generated with *evidence of randomness*
  - Publicly verifiable assurance that keys derived using a specified key generator
  - Prevents “trapdoors” (e.g., Crépeau-Slakmon), “weak” primes
- Research prototype stage

RSA-KEGVER & PKCS #11

- RSA Laboratories encourages consideration for high-assurance tokens
- PKCS #11 supports RSA key generation, but not “evidence”
- **Recommendation:**
  - Add “evidence” field
  - Add RSA-KEGVER (or other methods) as research matures into products, standards

Summary of Recommendations

- RSA-PSS: Add SHA-256+ versions to PKCS #11 v2.20
- RSA-KEM: Add as PKCS #1 etc. updated
- RSA-KEGVER: Add “evidence” field, add methods as research matures

Algorithm Strategy

- The bigger picture
- PKCS #11 supports a lot of algorithms already, and there are many more in other standards
  - IETF, NIST “schemes”, NESSIE, …
- How to decide which ones to add?
- ANS X9.44 strategy: *Reflect & guide*

Reflect & Guide

- *Reflect*: Support methods employed in industry, profiled for better security
- *Guide*: Add methods with better security, adapted to integrate with industry practice
- Examples in draft ANS X9.44:
  - Reflect: Existing TLS handshake
  - Guide: Revised handshake using RSA-KEM

Next Steps

- Choose new mechanisms
  - which ones?
- Draft text for PKCS #11
- Consider the algorithm strategy
- Add other mechanisms to implement strategy

Contact Information

- Burt Kaliski
  RSA Laboratories
  bkaliski@rsasecurity.com
  +1 781 515 7073