HMAC-authenticated Diffie-Hellman for MIKEY

IETF #53 Minneapolis 2002

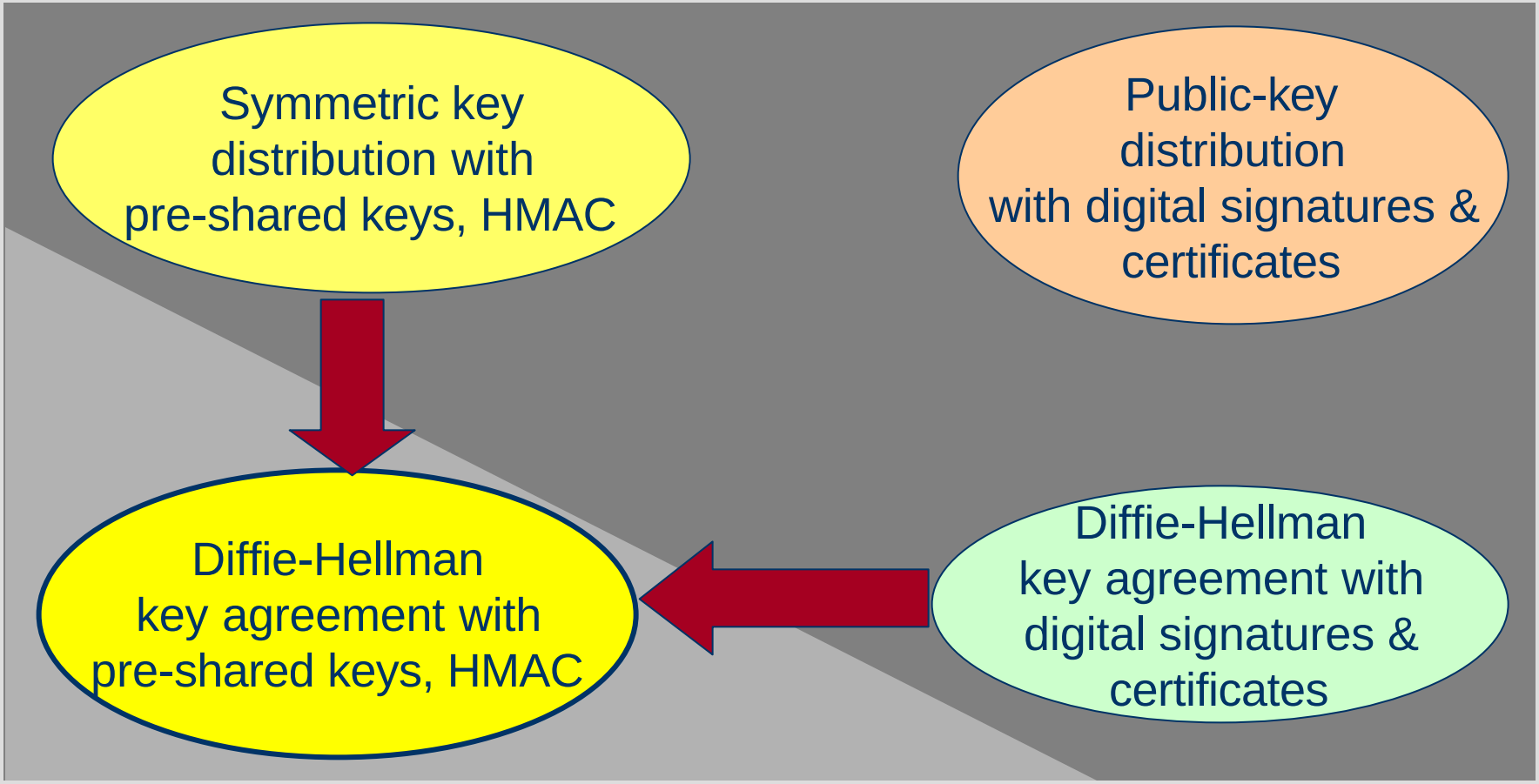
SIEMENS

Information
and Communication
Networks

Dipl.-Inform. Martin Euchner
Siemens AG, Information & Communication Networks, M SR 3
81359 Munich, Germany
Tel: +49 89 722 55790 E-mail: martin.euchner@icn.siemens.de

draft-euchner-MIKEY-DHHMAC-00.txt

MIKEY Key Management Protocols



- peer-to-peer
- 1 round trip

SIEMENS

DH-HMAC

- Scenario:
  - Point-to-point groups,
    pre-shared symmetric authentication key available
  - Independent of a PKI
  - Quasi-synchronized time clocks
  - Real-time key management requirements (secure VoIP)

- Idea and Approach:
  - Replace digital signature with keyed HMAC
    Use symmetric authentication key for mutual authentication of DH-half keys; eliminate certificates
  - HMAC-SHA1 provides high-performance security
    - default 160 bit digest
    - optional truncated 96 bit digest for reduced bandwidth
  - DH-HMAC payload types defined for integration into MIKEY
  - Simple implementation without additional mechanisms.

SIEMENS

DH-HMAC Security Protocol

A	B

$I := (ID_A)$

$K := g^x \bmod p \;||\; T \;[||\; I]$

$A := HMAC(auth\text{-}key, K)$

K, A

$I' := (ID_B)$

$K' := g^y \bmod p \;||\; T \;[||\; I']$

$B' := HMAC(auth\text{-}key, K')$

K', B'

$k_p := g^{xy} \bmod p$

$k_p := g^{xy} \bmod p$

SIEMENS

Comparison

Symmetric key distribution:

- − not scaleable to larger configurations but acceptable in small-sized groups
- − no perfect forward secrecy
- − key generation just by the initiator
- \+ no dependency on a PKI
- \+ high-performance, low bandwidth
- \+ simple & straight-forward master key provisioning

Public-key encrypted:

- − depends on PKI for full scaleability
- − expensive, non-real time certificate validation
- − complexity of X.509/RSA standards
- − key generation just by the initiator
- − no perfect forward secrecy
- ± self-signed certificates would avoid PKI ⇒ limited scaleability, complex provisioning

DH-HMAC:

- − Scales just to point-to-point groups
- \+ fair, mutual key agreement
- \+ perfect forward secrecy
- \+ no dependency on a PKI and PKI standards
- \+ sound performance, reduced bandwidth
- \+ simple & straight-forward master key provisioning

DH-SIGN:

- − Scales just to point-to-point groups
- − depends on PKI for full scaleability
- − limited performance
- − expensive, non-real time certificate validation
- − complexity of X.509/RSA standards
- ± self-signed certificates would avoid PKI ⇒ limited scaleability , complex provisioning
- \+ fair, mutual key agreement
- \+ perfect forward secrecy

SIEMENS

Conclusion

- Each of the four key management protocols has its own merits but also drawbacks.
- There is no single ideal solution.
- None of the variants is able to subsume the other remaining variants.
- DH-HMAC features useful security and performance properties that none of the other 3 MIKEY variants is able to provide.

SIEMENS

IPR Statement

- This presentation may contain material covered by IPRs. Siemens has made provisions to enable the IETF to consider such material in standards discussions.

- Please see:

  http://www.ietf.org/ietf/IPR/SIEMENS-General