DH POP Algorithms BIS

Jim Schaad
August Cellars
Original Document

- Two methods of computing Diffie-Helman “signatures”
- Static DH-POP Signature
  - Key Agree Operation + HMAC-SHA1
- Discrete Logarithm Signature
  - Extend DH-SHA1 Signatures for longer groups
Update Static DH-POP

• Parameterize the description
  – KDF function – Was SHA-1
  – MAC function – Was HMAC-SHA1

• Define new OIDs for
  – dhPop-static-sha256-hmac-sha256
  – dhPop-static-sha512-hmac-sha512 (if desired)
New Static ECDH-POP

• Same algorithm as DH-POP but with EC
  – Must have same parameters as other side
  – Select KDF
  – Select MAC
  – Run MAC over data to be “signed”

• Suggested values
  – EC + SHA256 + HMAC-SHA256
  – EC + SHA512 + HMAC-SHA512
Update Discrete Logarithm Signature

• Parameterize the description
  – Hash algorithm – was SHA-1
• Define new OIDs for
  – Id-alg-dh-pop-SHA2
Questions

1. Adopt as working group item?
2. Add other algorithms?
3. EC Discrete Logarithm Signature?