HMAC-authenticated Diffie-Hellman for MIKEY

IETF #55 Atlanta 2002

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

draft-ietf-msec-MIKEY-DHHMAC-00.txt

Background

- In IETF#53 (Minneapolis) comparison was made among the 3 MIKEY security protocols
  - Symmetric key distribution
  - Public-key encrypted
  - DH-SIGN

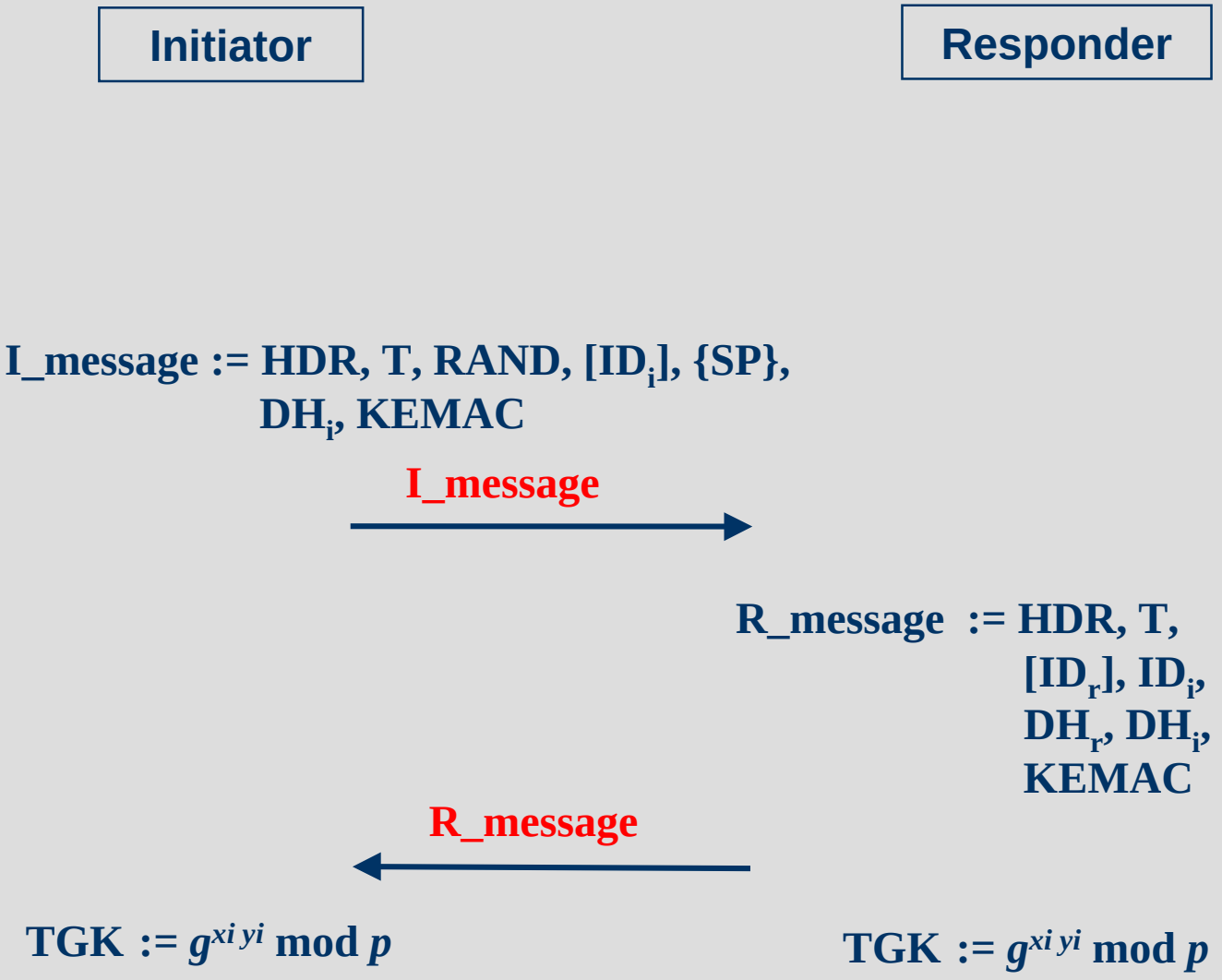
  and new proposed DH-HMAC

  w.r.t. performance, security, PKI dependency and provisioning
- Conclusions:
  - There is no single ideal solution. Each of the four key management protocols has its own merits but also drawbacks
  - 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.

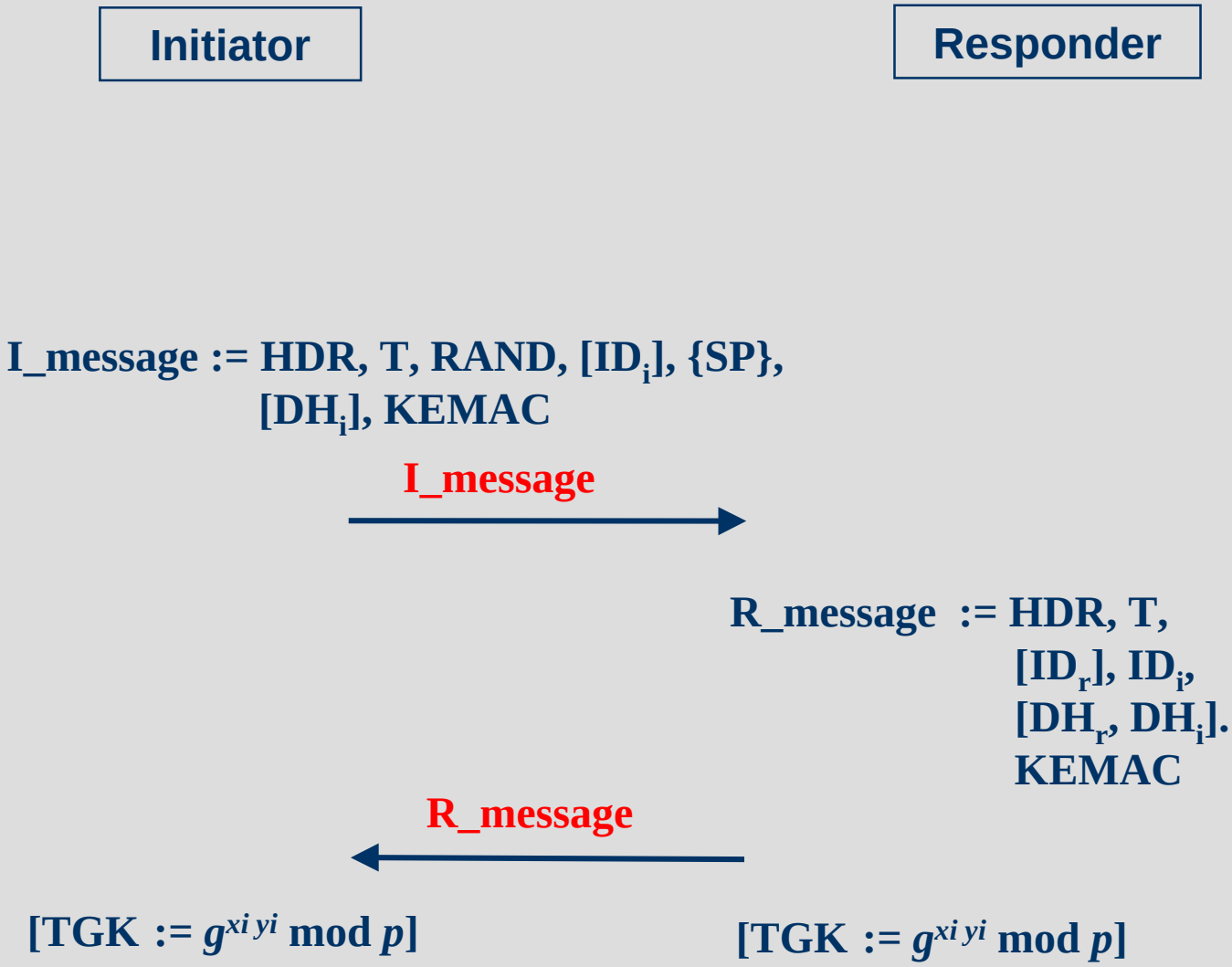
Changes against draft-euchner-MIKEY-DHHMAC-00.txt

- Made a MSEC WG draft
- Aligned with MIKEY-03 DH protocol, with notation and with payload formats
- Clarified that truncated HMAC actually truncates the HMAC result rather than the SHA1 intermediate value.
- Improved security considerations section completely rewritten
- IANA consideration section added
- A few editorial improvements and corrections
- Suggested as Informational RFC/**Proposed Standard**
- IPR clarified and IPR section changed

DH-HMAC Security Protocol



DH-HMAC TGK re-keying Security Protocol



Security Considerations Section

- Section completely rewritten in the spirit of:
  E. Rescorla, B. Korver:
  "Guidelines for Writing RFC Text on Security Considerations".

- Issues addressed:
  - Security environment
  - Threat model
  - Security features and properties
  - Assumptions
  - Residual risk

Threat model

Threats of concern:

- Unauthorized interception of plain TGKs.
- Eavesdropping of other, transmitted keying information
- Masquerade of either entity
- Man-in-the-middle attacks
- Loss of integrity

Threats not in scope:

- Passive and off-line cryptanalysis of the Diffie-Hellman algorithm
- Non-repudiation of the receipt or of the origin of the message
- Denial-of-service or distributed denial-of-service attacks.

Security features and properties

- Secure key agreement with the establishment of a TGK at both peers
- Peer-entity authentication (mutual)
- Cryptographic integrity check
- Replay protection
- Limited DoS protection
- Perfect-forward secrecy (PFS)
- Fair, mutual key contribution
- Efficiency and performance
- Security infrastructure
- NAT/Firewall-friendliness
- Scalability

Open Issues

- Enhance the MIKEY protocols by elliptic curve cryptography?
  - Provides improved performance and increased security for real-time critical applications
  - ⇨ Enhancements would not change the MIKEY security protocols
  - ⇨ but will introduce new payloads for EC-Signature (MIKEY only) and EC-DH (MIKEY and DHHMAC).
- Proposal:
  - ⇨ Define the ECC enhancements as an option to MIKEY and DHHMAC.

IPR Statement

- This presentation may contain material covered by IPRs.
- Siemens does not hold the related IPR anymore.
- The author is aware of related intellectual property rights currently being held by Infineon.
- Pursuant to the provisions of [RFC-2026], the author represents that he has disclosed the existence of any proprietary or intellectual property rights in the contribution that are reasonably and personally known to the author.
  The author does not represent that he personally knows of all potentially pertinent proprietary and intellectual property rights owned or claimed by the organizations he represents or third parties.


Thank You!
It's time for Questions...

Backup: 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