

HMAC-authenticated Diffie-Hellman for MIKEY

IETF #56 San Francisco 2003

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-dhmac-01.txt

Update

Changes against –00.txt

- category set to proposed standard.
- identity protection clarified.
- aligned with MIKEY-06 DH protocol, with notation and with payload
- some editorials and nits.

Next Steps

- Document ready for WG LC?

Thank You!

It's time for questions...