EAP GPSK

Charles Clancy
Hannes Tschofenig

IETF 72
Dublin, Ireland
1 August 2008
EAP-GPSK

• Minor changes since the last revision
  – Address Pasi's review

• Single issue remains: MAC input vs output length
  – Draft assumes that key lengths for MAC are the same as the MAC output length, and states this constraint
  – Counterexample: AES-CMAC-256
    • 256-bit key for AES
    • 128-bit output
  – Do we care?