

# JOSE Cookbook

Matt Miller

IETF 91 - Honolulu

# Changes from WGLC

- Fixes to terminology
- UNICODE password
- Section on JWKs

# On JWKSs

- Public vs. Private
  - EC, RSA
- Length expectations
  - EC, RSA, oct
- Padding expectations
  - EC, oct
  - ! RSA

# Next Steps

- In AD Evaluation
- Include semi-compact JSON examples
- Editorial nits