

# Generalized Key Distribution Extensions

Charles E. Perkins/Nokia

Pat R. Calhoun/Sun

# Keys for use with Foreign Agent

- All keys considered for use when creating authentication data for Mobile IP registration messages and Binding Updates
- Useful for smooth handovers
- Useful for regional registrations
- Needed for method in Registration Keys draft

# Variations

- Different Extensions for Request and for Reply
- Extension type depends on use of key
- Currently in document:
  - MN-FA Request and Reply
  - MN-HA Reply
  - FA-HA Reply
- Different subtypes for source of the key

# Issues

- Lifetime field for generalized MN-FA extension
  - (or, is it part of particular subtype data?)
- Should similar idea be used for privacy keys?
- Should FA-HA Request be included?
- Should MN-HA Request be included?
  - (or is this always implicit?)
  - would cost more bandwidth over the air