

TF-Mobility Meeting  
RadSec 20 September 2006



# RFC for RadSec

# Background



- discussions in TF-Mobility and for GN2 deliverable DJ5.1.4 triggered the RadSec specification idea
- some e-mail exchange with people from the IETF radius extensions working group
- result: write an I-D that describes existing implementations
- two implementations:
  - Radiator from Open System Consultants
  - FreeRADIUS (in progress)

# Transport Profile



- transport profile: TCP only  
(SCTP still too far away from serious deployments)
- agreement: keep connections alive for entire instance lifetime
- How to achieve that?
  - TCP socket options? Not alone: too OS-specific, no influence from application layer, not available on all platforms
  - application-layer keepalive packet? more control, but more complicated to implement  
DeKok's idea: use the existing Status-Server

# Keepalive



- most existing RADIUS implementations have support for that
- not RFCed anywhere
- Alan DeKok writes an own Internet Draft to document Status-Server usage  
( one server sends Status-Server, other replies with correctly authenticated Access-Accept and Reply-Message with status details)
- OSC is in favor of keeping socket options
- compromise: in any case reply to Status-Server, and SHOULD send yourself
- socket options can additionally be used

# TLS



- OSC whitepaper specified TLSv1 (in 2005)
- TLSv1 was obsoleted by TLSv1.1 in 2006
- according to OSC, TLSv1.1 will be used in recent installations
- so: probably, TLSv1.1 will be mandatory in the spec
- include in spec that cert verification might not just rely on the CN, but arbitrary fields in the cert (such as our URN)

# Open Questions



- one connection bidirectionally?
- or rather one for each direction?
  
- failover/failback: use a reply-time based (simple) algorithm?
  - measure response times between Status-Server and its Access-Accept
  - not yet received responses count as `received==NOW()`
  - connection with the smaller reply-time wins
  - of course only on servers that are not authentication leaves

---

# The End

