# SSLS for DOTS Security

Providing Security above Transport

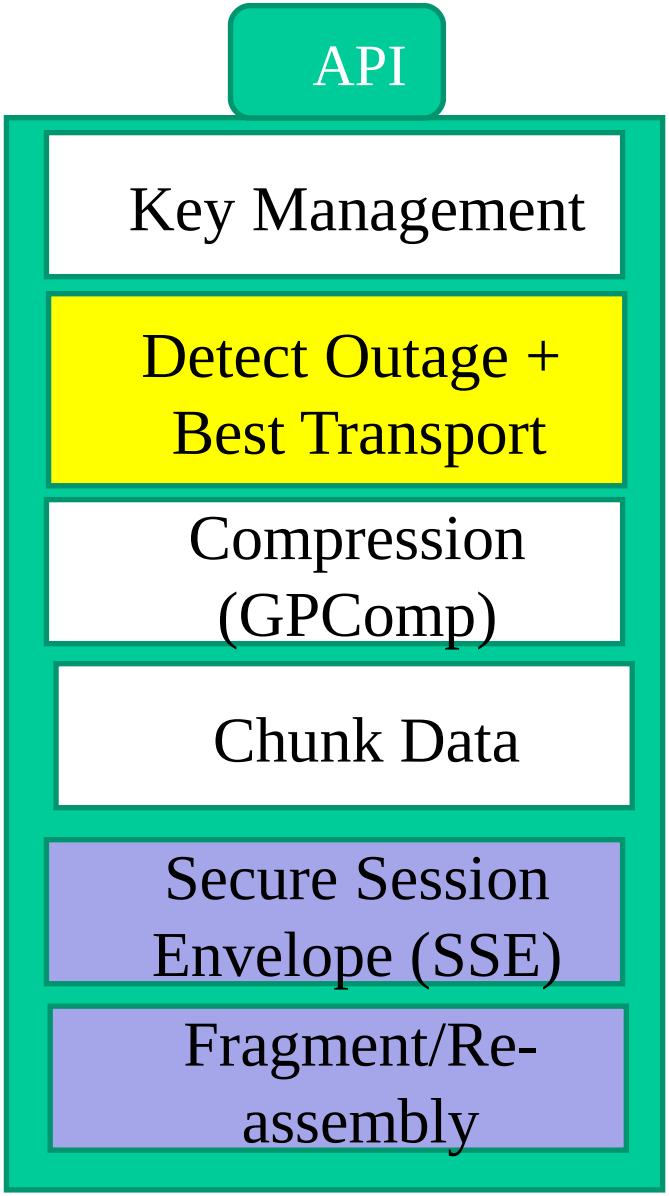
IETF 95
Buenos Aries, AR
April 8, 2016

Robert Moskowitz
HTT Consulting

draft-moskowitz-dots-ssls-02.txt

# What is SSLS?

- Secure Session Layer Services
- Introduces an OSI-styled session service
  - Independent of underlying transport services
- Offers a set of services to an application
  - Chunking
  - Security
  - Compression
  - Fragmentation / Reassembly
- Peer KMP negotiates services
  - e.g. IKE or HIP



# Why SSLS

- Differing circumstances may benefit from differing transport for DOTS messages
  - TCP, UDP, SMS
- Fate-sharing between security and transport offers a cheap attack surface.
- Peer KMP makes recovery clearer where either agent can restart security context.

# What SSLS services not needed

- Chunking
  - DOTS messages not indeterministic like NETCONF
- Compression
  - DOTS messages already small, nothing gained by trying to compress
- Fragmentation/reassembly
  - Not for UDP, as messages small enough
  - Maybe for SMS

# So what is SSLS providing

- Secure Session Envelope (SSE)
  - Basically ESP moved above Transport
  - Smaller header compared to ESP
  - KMP is IKEv2 or HIPv2 (or DEX)
    - Peer KMP allows either agent to start/restart
    - SA can survive reboot if stored properly

# But SSLS is new

- Can use IKEv2
  - Over UDP for NAT traversal
- NetBSD API example available
- Operational benefits make it worth the development

# DISCUSSION