Guidelines for the use of the SIPS URI Scheme in SIP

draft-audet-sip-sips-guidelines-04

François Audet - audet@nortel.com

Status (from Chair)

- Candidate: Informational
- Milestone for WGLC March 2007
- Milestone for submission to IESG June 2007
- This was agreed to be a working group document at IETF #67
- The document is INFORMATIONAL. It does not update RFC 3261. It will describe two things:
  - If we use SIP security mechanisms as defined now, this is what you will get.
  - It will examine the options for improvement, from which the WG can make informed decisions about changes necessary. The protocol changes will not appear in this document, but will be the subject of other documents, and we will need to recharter to add milestones when we do this.
  - Any proposed changes can be
    - BCP (i.e. the current rules in RFC 3261 are best used – should only be used - in the following manner to achieve a desired result), or
    - standards track (updates RFC 3261) to change the rules or make new normative statements about security, or to include new mechanisms.

Summary of Changes from -02 version

- Routing & Registration
  - sip:audet@example.com and sips:audet@example resource refer to the same resource, audet@example.com
  - Does NOT explicitely list transport and both sip and sips when registering: huge simplification
  - Mechanical rules for usage of SIP or SIPS in Registration
  - It is the association of the Contact in REGISTER with the AoR that will determine if the user is reachable or not with SIPS URI

Summary of Changes

- Clarified meaning of sips
- Use of dual Record-Route entries to deal with upgrading/downgrading between SIPS SIP on a hop
- Call flows were completely rewritten as a result, and are now very extensive
- Lots of maintenance

Dean’s sips trial balloon proposal

- BCP for Secure Operation: 4 major points
    1. Implementations SHOULD use TLS for SIP transport using sip:. MAY use IPsec instead, or others, MUST have adequate level of security
    2. When using sips:, MUST not exercise “last hop exception rule”
    3. Use sip: instead of sips: for best-effort SIP over TLS
    4. Sips: termination MUST use Sips for all derived connection. Does NOT allow PSTN termination of sips:

To do

- Please look at To-Do list, provide suggestions
- Do we need new mechanisms, and why?
- Do we need to deprecate sips? Need rationale