Guidelines for the use of the SIPS URI Scheme in SIP

draft-audet-sip-sips-guidelines-02

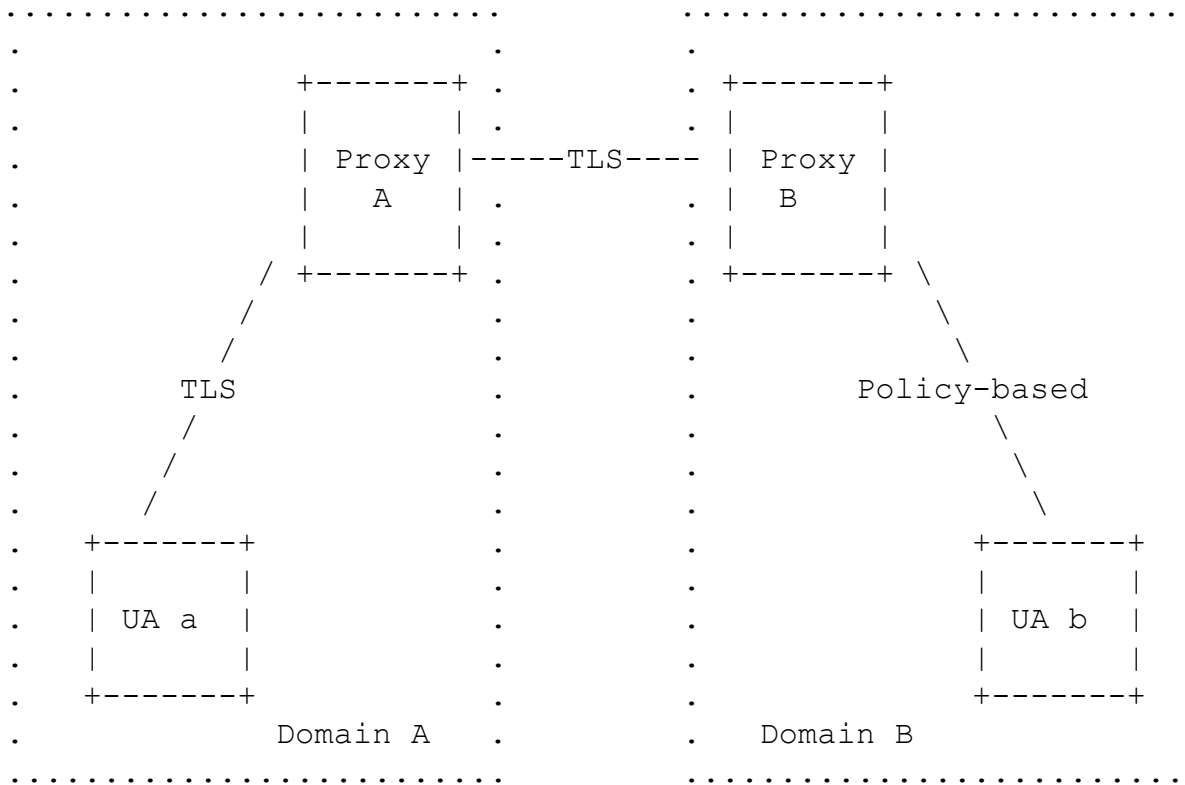François Audet - audet@nortel.com

Status and Background

- Started the wacky thread of the month!
- Usage of SIPS scheme is, at best, "underspecified" in RFC 3261
- Draft attempts to "explain" RFC 3261
- 3rd iteration of individual draft, based on email list discussion
- Lots of feedback from developers and list
  - Sense of urgency
- Goal: WG document

Draft content

- Meaning of SIPS
- Upgrading and downgrading between sip/sips
- Usage of SIPS in Registration
- SIPS in a dialog
- Usage of transport=tls and Via TLS parameters
- REFER, Routing, GRUU, outbound, background

Meaning of SIPS and dialog

- RFC 3261: TLS for each hop, until reaching terminating domain

```
.............................              .............................
.                           .              .                           .
.             +-------+     .              .     +-------+             .
.             |       |     .              .     |       |             .
.             | Proxy |-----TLS----        |     | Proxy |             .
.             |   A   |     .              .     |   B   |             .
.             |       |     .              .     |       |             .
.          /  +-------+     .              .     +-------+  \          .
.         /                 .              .                 \         .
.        /                  .              .                  \        .
.      TLS                  .              .            Policy-based   .
.      /                    .              .                    \      .
.     /                     .              .                     \     .
.    /                      .              .                      \    .
.  +-------+                .              .                +-------+  .
.  |       |                .              .                |       |  .
.  | UA a  |                .              .                | UA b  |  .
.  |       |                .              .                |       |  .
.  +-------+                .              .                +-------+  .
.             Domain A      .              .      Domain B             .
.                           .              .                           .
.............................              .............................
```

Meaning of sips

- Does not mean a "Padlock" icon

- Issues:

    – Creates problems in reverse path because first hop becomes last hop

    – Also, when Record-route is not used, using sips in Contact is very dangerous

Meaning of sips

- Suggestions from the list
    1. Deprecate SIPS altogether
    2. Deprecate "last hop exception" (not sufficient in itself)
    3. Explain the exception, and fix bugs it creates
- Draft assumes 3, but description of possible fixes is not done yet
- Lots of people like 2
    - Need to accommodate 3GPP

Dialog: Potential Solution (3)

- Allow for transport=tls as a contact in a dialog?
  - Formally deprecated in RFC 3261, but most people disagree that it's "really" deprecated (be pragmatic)
  - Allows for "best effort" hop-by-hop usage of TLS
  - A UA that doesn't understand the parameter will ignore it
- From the list: add a transport=tls-sctp (like Via)

Registration: AOR

- Use SIPS when ONLY SIPS is valid (always secure) – does not imply SIP
- Use SIP otherwise
- SIP implies SIPS:
    - Big issue since many, if not all, UAs can not process SIPS URIs
    - Do we need a way to explicitly register sip only?
        - New parameter in To?
        - Inferred from Contact? (sip vs. sips?)

Registration: Contacts

- Lists explicitly all valid transport (UDP, TCP, TLS, …)

- Use q-value

- Should we use transport=tls parameter instead of overloading "sips"?

  - All known implementations do this for "best effort" TLS