SIPconnect 2.0

Andrew Hutton - @huttonandy
Atos Distinguished Expert & SIP Forum Director

unify
atos collaboration solutions

https://twitter.com/huttonandy

Background

SIPconnect 2.0

- SIPconnect defines SIP Service Provider to SIP-PBX interface
- SIPconnect 1.0 approved in January 2008
- SIPconnect 1.1 approved in May 2011
- SIPconnect 2.0 approved in December 2016
  - Wow - that was less than a year ago.
- 2.0 Editors: Andrew Hutton, Nils Hänström, Gonzalo Salgueiro
- Disclaimer – These slides don’t list all the differences between SIPconnect1.1 and 2.0.

Background

SIPconnect 2.0

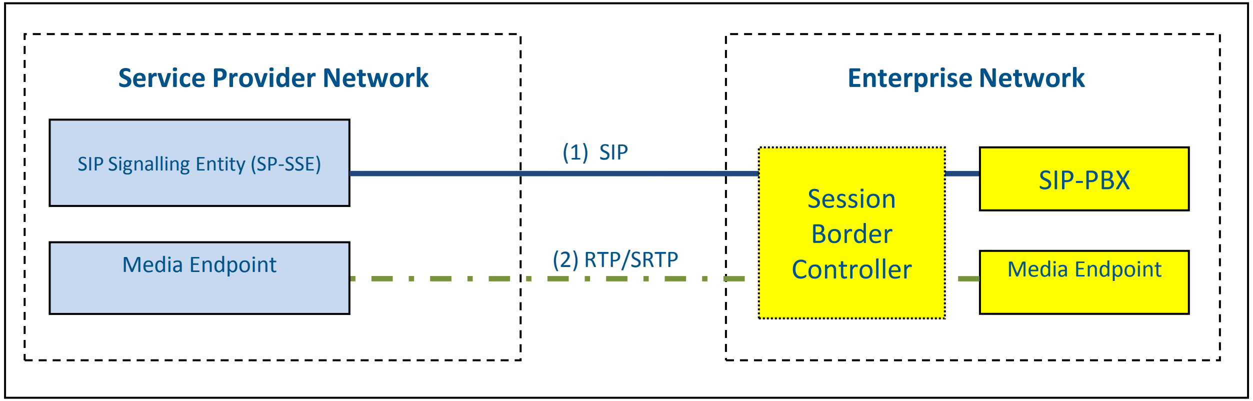
SIP FORUM

IETF

SIPconnect 2.0 – Charter

- ❖ Update the reference architecture (E.g. to include SBC's).
- ❖ Specify the exact RFCs or other existing standards associated with these protocols that must or should be supported by each element of the reference architecture.
- ❖ Update the security model.
- ❖ Specify the consensus method for supporting secure media (SRTP).
- ❖ Specify the consensus method for supporting Video enabled devices.
- ❖ Specify the consensus method for supporting IPV6 Single IP and IPV4/6 Dual IP Dual Stack components within the reference architecture.
- ❖ Specify the consensus method for supporting emergency calling (NG911/NG112) and the transport of location information.

Update the Reference Architecture – SBC's



- SIPconnect includes signaling and media interfaces.
- SIPconnect2.0 – Points to RFC 7092 (IETF STRAW) on B2BUA Taxonomy – describes ways in which elements can be combined.
- However Enterprise Network still a black box for conformance.

SIP Security (TLS) – Not SIPS

- New sections provide more details on SP-SSE (8.1.1) and SIP-PBX (8.1.2) requirements.
- MUST Support TLS 1.2 and MAY support higher versions when available.
- Cipher Suite requirements.

An SP-SSE **MUST** support the following cipher suite:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256.

The SP-SSE **MAY** support the following cipher suites for backwards compatibility:

- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA

- Both SIP-PBX and SP-SSE SHOULD verify the status of a certificate received during TLS establishment. It is RECOMMENDED to use OCSP Stapling ([RFC 6066] and [RFC 6961]).
- Some issues raised that there is gap in standards regarding SP-SSE requirements for selecting TLS connection to SIP-PBX – Lack of requirements/implementations of SIP Outbound – To be discussed in IETF.

SIP Media Security (SRTP)

- New section 14.4 includes a profile for Secure RTP (SRTP).
- SIPconnect 2.0 Media Endpoints SHOULD secure the media using SRTP [RFC 3711] and when doing so MUST use SDP Security Descriptions (SDES) [RFC 4568] for the necessary key exchange.
- Also includes guidance on crypto-suites to use and what RFC 4568 parameters to use.
- RFC 4568 – Security Descriptions is currently the most common key exchange mechanism implemented and deployed in SIP endpoints.
- SIPconnect 2.0 does not include a best effort approach (negotiated) to SRTP it is either on or off by configuration.
  - This is due to lack of standards and we have taken this to the IETF (https://tools.ietf.org/html/draft-ietf-sipbrandy-osrtp-02 and https://tools.ietf.org/html/draft-ietf-mmusic-opportunistic-negotiation-01)
- We will need to watch IETF work on SIP media/privacy best practice (SIPBRANDY / MMUSIC Working Group) and maybe adapt in the future.

SIPconnect2.0 and IPv6

- New section 15 describes IPv6 requirements.
- For the sake of simplicity and to avoid interoperability issues, neither the Service Provider nor the Enterprise is required to support a dual stack implementation. In particular, media negotiations via ICE (RFC 5245), ALTC (RFC 6947), or similar mechanisms are out of scope.
- The same IP Address family must be used for both signaling and media.
- An Enterprise MAY split its subscribers between an IPv4-connected network and an IPv6-connected network; however, this split must be considered as two separate instances of the SIPconnect interface.
- The decision not to require dual-stack based on simplicity and the recognition that SP-SSE's are unlikely to support both on the same interface.

Early Media and VoLTE Interworking.

- Section 14.9 (Ringback Tone, In-band Tones, and Early Media) Updated to include MAY strength requirement for the P-Early-Media header [RFC 5009].
- P-Early-Media used in VoLTE networks and is useful in solving some well known problems with early-media in SIP networks.
- Makes it clear when early-media is supported and can be used.

Emergency Calling and Location

- Added section 13.1 on Location Conveyance.
- What we could say is limited due to the fact that SIPconnect is used internationally and location conveyance requirements are the subject of local regulatory requirements.
- However we included guidance on the use of the SIP Geolocation Header field [RFC 6442] and when location is provided by value how it MUST be structured in accordance with the formats and rules defined in [RFC 5491] and transported in a PIDF-LO as defined in [RFC 4119].

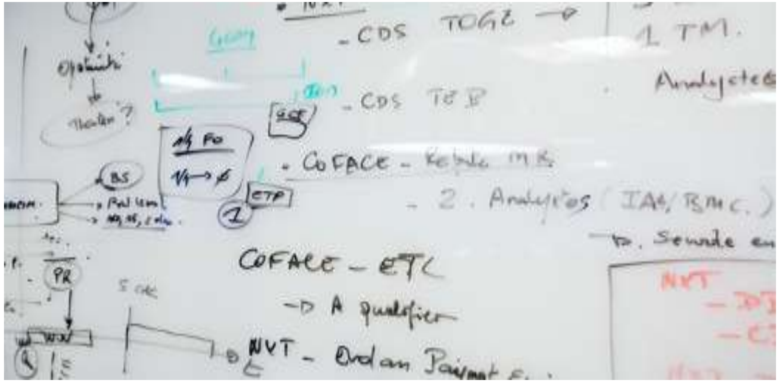
What happened to Video?

- Video was major driver for SIPconnect 2.0.
- We had planned to reference the IMTC BCP specifications on SIP Video & Sync with NNI Spec.
- However there has been a distinct lack of interest in adding Video to SIPconnect.
- Did WebRTC kill SIP trunking video?

What happens next?

- SIPconnect 2.0 released in December 2016.
  - Needs some time to mature and be adopted?
  - Certification Program – New stuff is mostly optional.

- SIPconnect Next Version.
  - STIR / SHAKEN Requirements?
  - Best Effort SRTP?
  - Video?
  - Your favourite requirement?



Thank You

Andrew Hutton - @huttonandy