SRTP Draft Status

56th IETF

Status

- In IESG Review
- Changes requested at last IETF
- More changes requested recently

Changes

- Craft precise language about when SRTP NULL authentication is acceptable and its risks
- Add text describing reflection and replay attacks
- Mandate 80-bit SRTCP authentication
- Make **80-bit** SRTP authentication the default
- Remove error tolerance from the spec, eliminating non-propagation of bit errors from the goals,
- Mandate automatic key generation/management
- Reflect recent feedback from programmers