Using SEED Cipher Algorithm with SRTP

draft-ietf-avt-seed-srtp-01.txt

Seokung Yoon (KISA)

The SEED Algorithm : Review

- developed by KISA in 1999
- Standard status
  - TTA Standard in Korea
  - IETF Standard & ISO/IEC Standard
- Feature
  - Block cipher with DES-like(Feistel) structure
  - The size of input/output bit is fixed 128-bit
  - A strong round function against known attacks

Changes since-00

- Define SEED-CM(Counter Mode) and SEED-CM PRF

  => SEED counter mode and SEED-CM PRF are defined in a similar manner, and are denoted as SEED-CM and SEED-CM PRF respectively. The only difference in the processing is that SEED-CM and SEED-CM PRF use SEED

- Remove padding and CBC mode in the draft

Changes since-00

- Modify SRTP Crypto Suites using SEED

Parameter	Value
SRTP and SRTCP encr transf.	SEED-CM
SRTP and SRTCP auth transf.	HMAC-SHA1
SRTP and SRTCP auth tag length	80 bits
Key derivation PRF	SEED-CM
Key material params (for each master key) :	
master key length	128 bits
n_e (encr session key length)	128 bits
n_a (auth session key length)	160 bits
master salt key length	112 bits
n_s (session salt key length)	112 bits
key lifetime	
SRTP-packets-max-lifetime	2^48
SRTCP-packets-max-lifetime	2^31

Next Step

- Questions or Comments??
- Ready for WGLC??