AVTCORE

Encrypted Key Transport

draft-ietf-avtcore-srtp-ekt-00
(previously draft-ietf-avt-srtp-ekt-03)

August 2, 2012

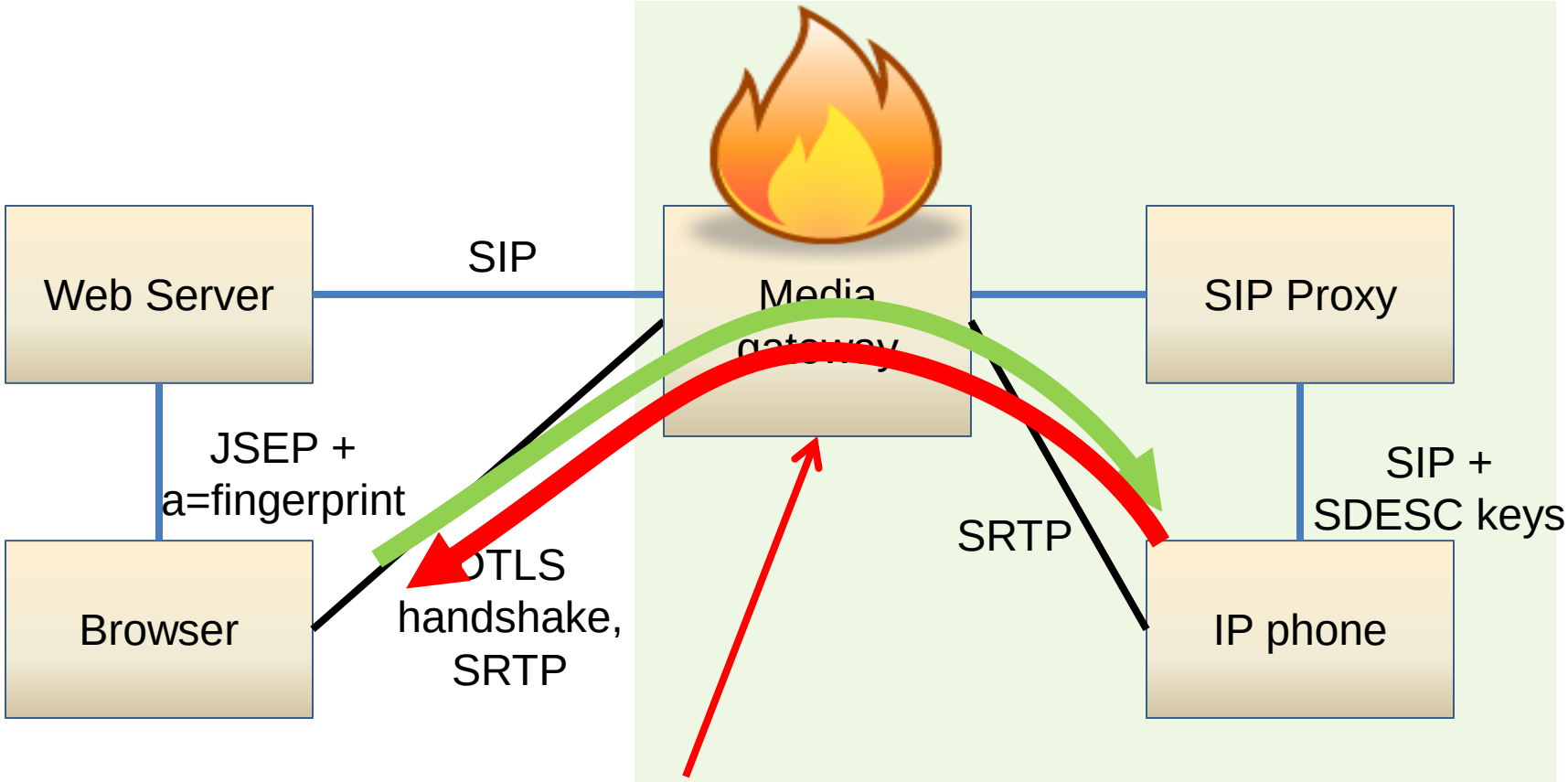
IETF-84, Vancouver

Authors: David McGrew, Flemming Andreasen, Dan Wing, Kai Fischer

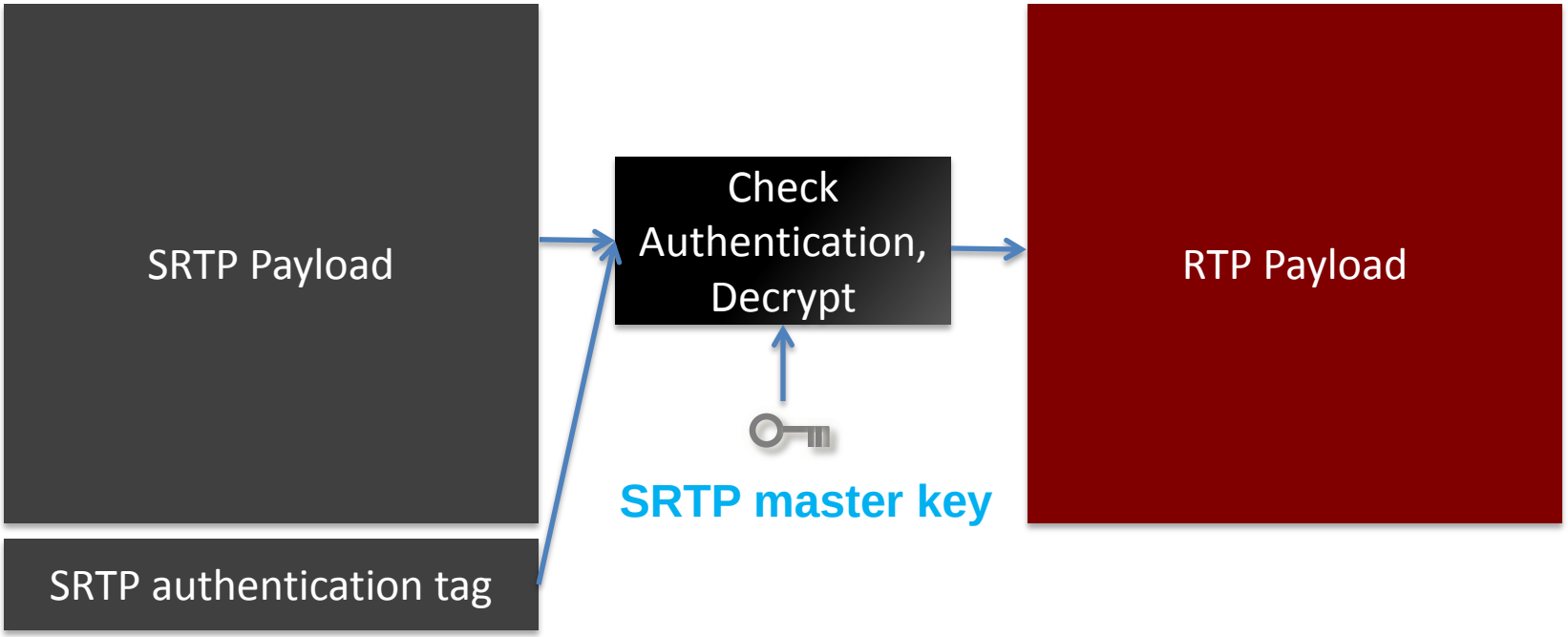
EKT for Interop

- Interoperate between Security Descriptions and EKT (e.g., DTLS-SRTP-EKT)
- Avoids per-packet SRTP cryptographic operations on gateway
- EKT tag now independent of SRTP packet
  - Media gateway can add/remove EKT tag to/from SRTP packet, resulting in normal SRTP packet
  - Implementation and security analysis simpler

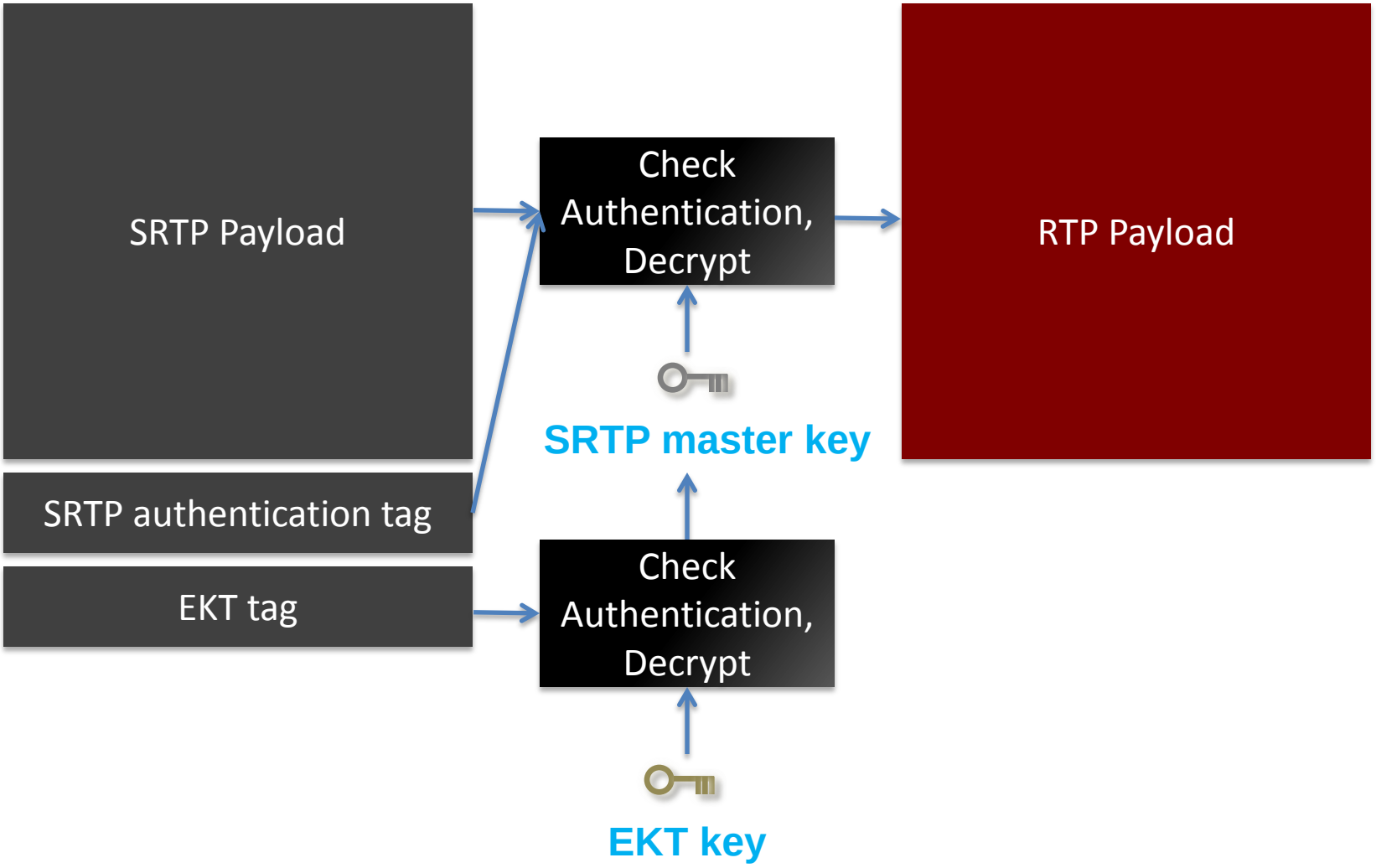
Previous situation



How SRTP decryption works

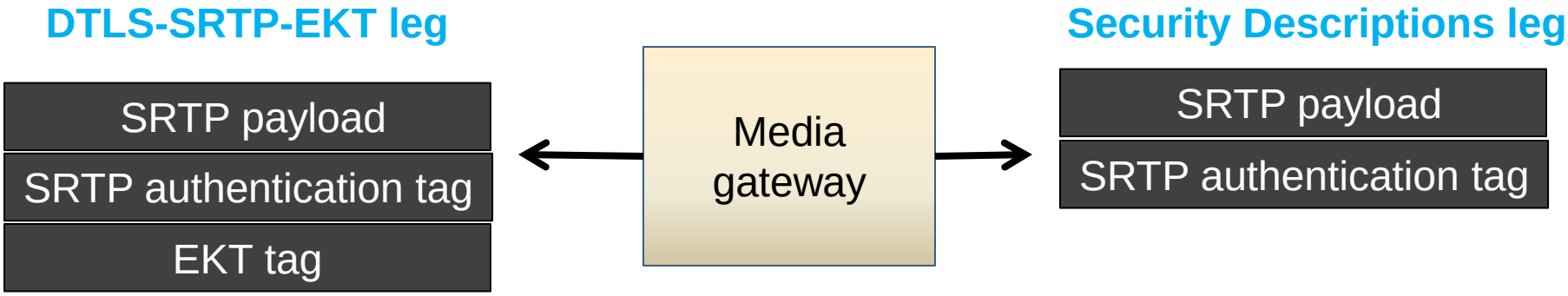


How EKT decryption works

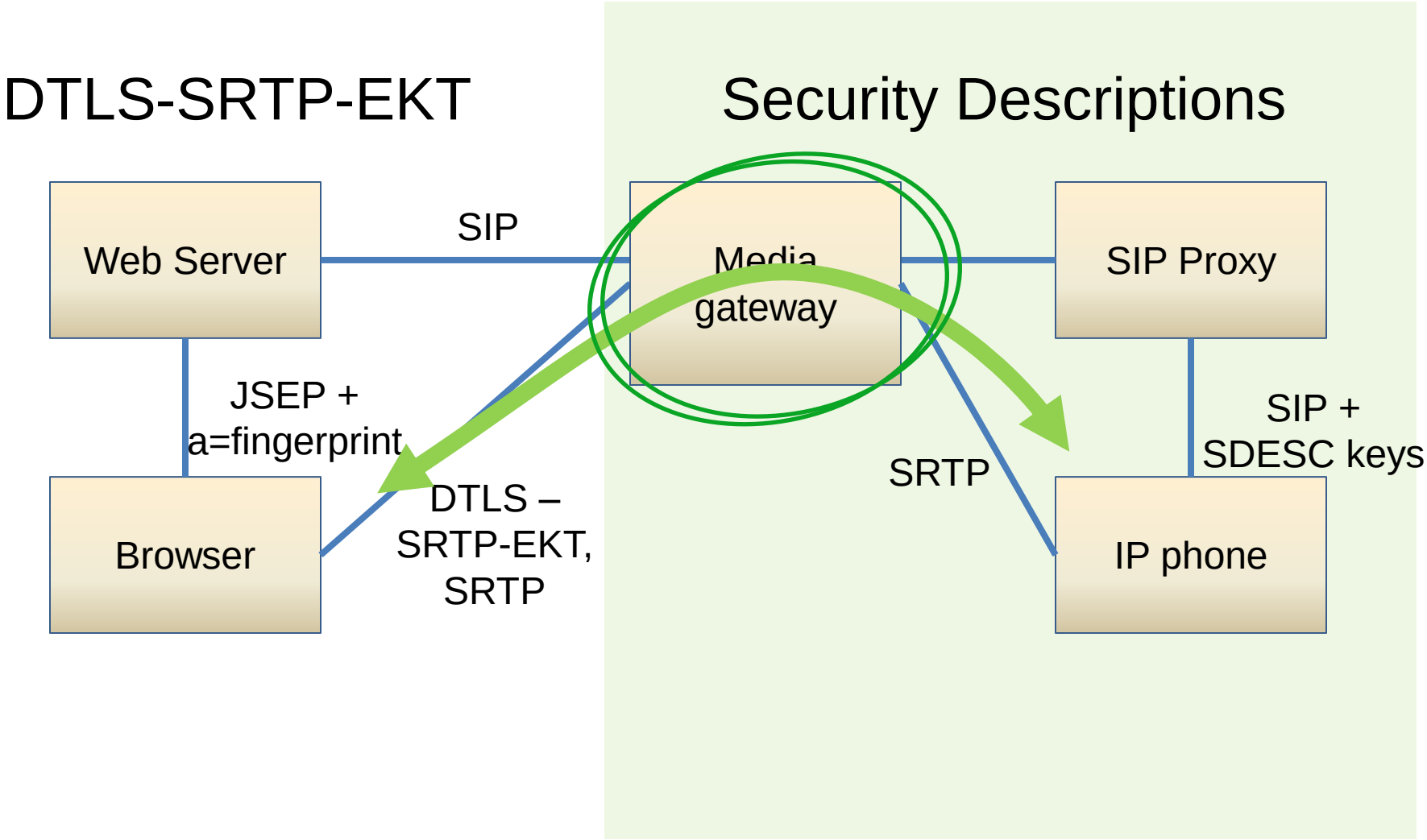


Enhancement to EKT for Interop

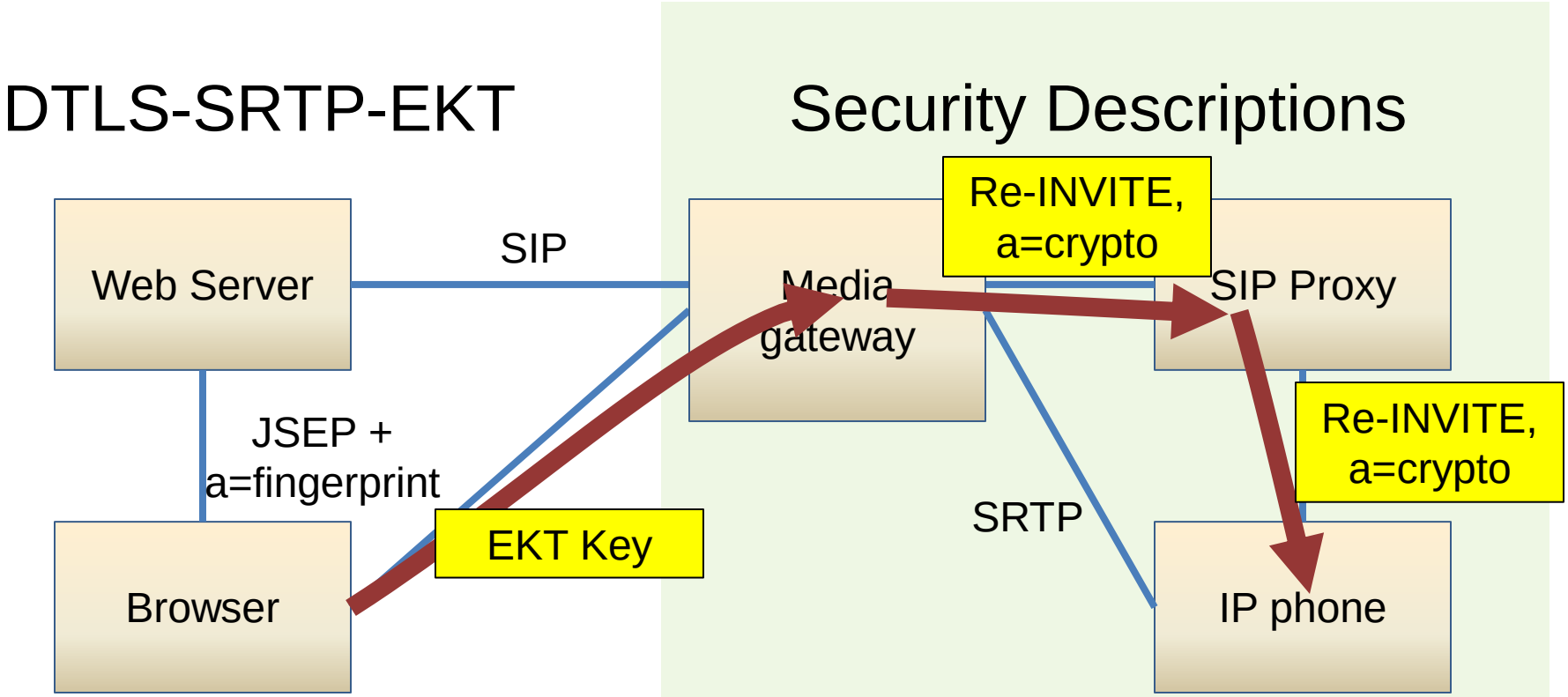
- Adds to SRTP without changing SRTP format or processing rules
  - **EKT tag is now removable**
- Benefit: Easy for media gateway interoperation



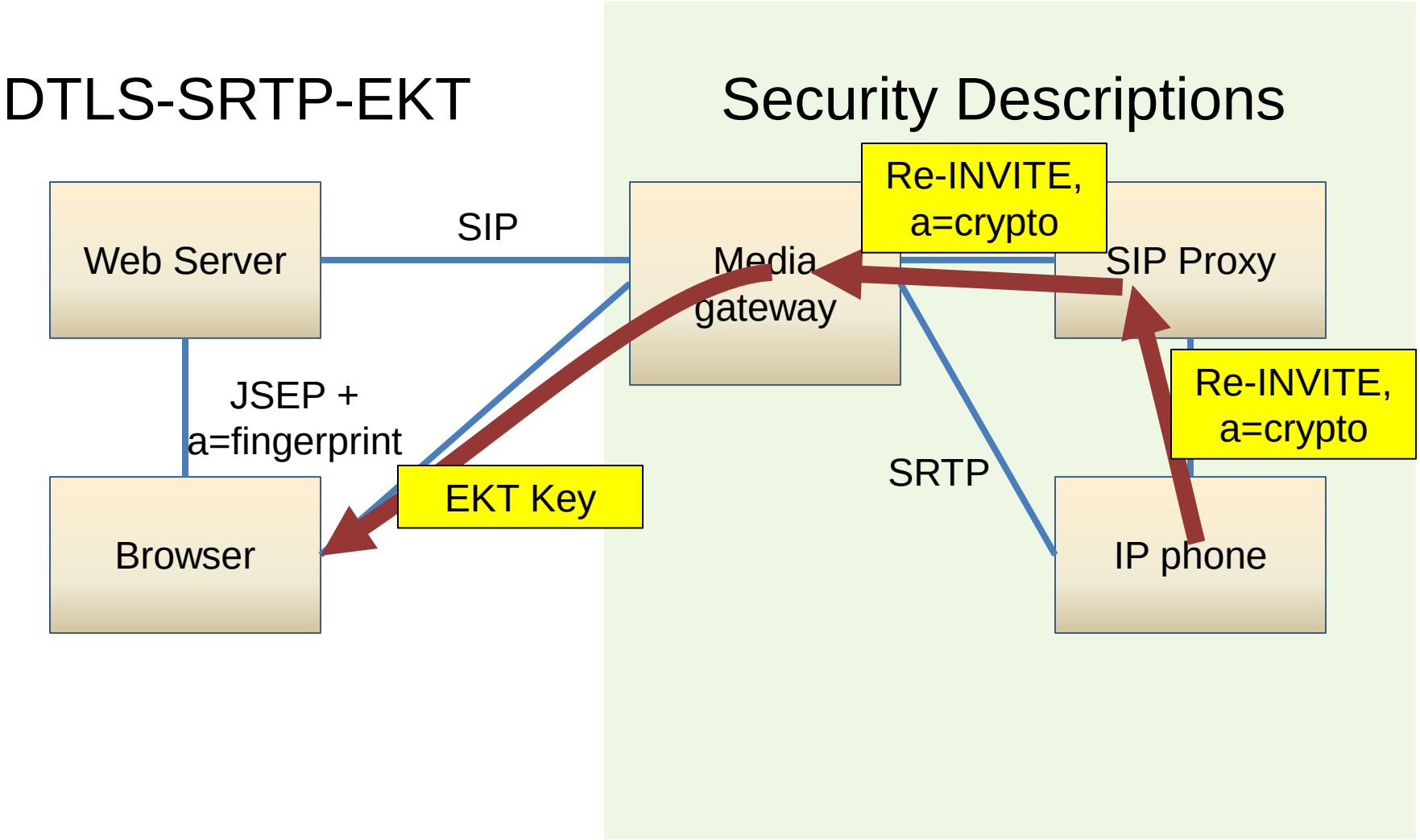
DTLS-SRTP-EKT and Security Descriptions Interop



Key Changes from EKT



Key Change from SDES



End