RTCWEB Working Group

Media Security:
A chat about RTP, SRTP, Security Descriptions, DTLS-SRTP, EKT, the past and the future

Dan Wing
dwing@cisco.com

IETF83 - March 2012

Agenda

- Scope
- Upcoming Questions for Working Group
- RTP versus SRTP
  - RTP, Recording, RTP versus SRTP
- Keying
  - Intro to Security Descriptions & DTLS-SRTP
  - Interworking SDESC and DTLS-SRTP using EKT
- Working Group Discussion

Purpose of This Presentation

- DTLS-SRTP is best path forward
- DTLS-SRTP meets RTCWEB's technical requirements
  - Interoperation with existing SIP endpoints
  - Best security we know how to build
  - Allows adding identity

Reading List: Keying Mechanisms (1/3)

- Security Descriptions, RFC4568
  - Sends SRTP session key over SIP signaling
  - Also called SDES or SDESC
- DTLS-SRTP, RFC5763 and RFC5764
  - DTLS on media path establishes SRTP session key
- EKT, Encrypted Key Transport, draft-ietf-avt-srtp-ekt
  - Group keying (and interoperation!)

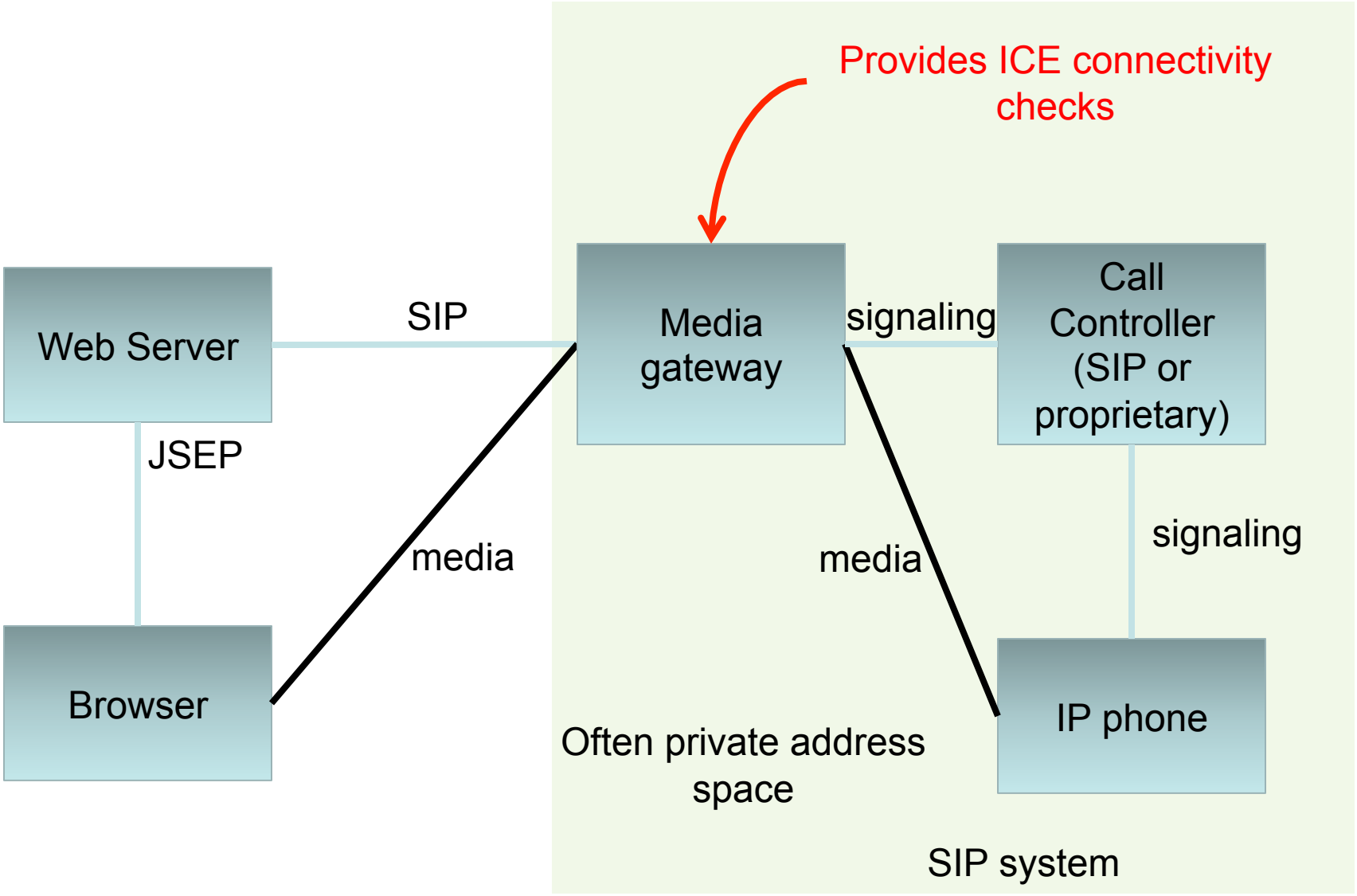
Reading List: Analysis of Keying Mechanisms (2/3)

- Requirements and Analysis of Media Security Management Protocols, RFC5479
  - Analyzed 15 SRTP keying mechanisms
  - Many criteria: SIP forking, retargeting, call signaling versus media path, group keying
  - Conclusion: best keying mechanism: DTLS-SRTP
  - (Most deployed is Security Descriptions)
    - more on that later

Reading List: Identity (3/3)

- SIP Identity, RFC4474
  - Signs certain SIP headers and entire SDP
- SIP Identity using Media Path, draft-wing-rtcweb-identity-media/draft-wing-rtcweb-identity-media (2007)
  - Signs certain SIP headers and a=fingerprint
  - DTLS handshake and identity signature proves identity
  - Cisco IPR statement, https://datatracker.ietf.org/ipr/1709

Model


Provides ICE connectivity checks
Web Server
SIP
Media gateway
signaling
Call Controller (SIP or proprietary)
JSEP
media
media
signaling
Browser
IP phone
Often private address space
SIP system

QUESTIONS FOR WORKING GROUP

Questions for Working Group

- At end of meeting, chairs will ask questions **similar to**:
  - Should we allow RTP?
  - For SRTP keying:
    - Do we need Security Descriptions?

RTP VERSUS SRTP

RTP

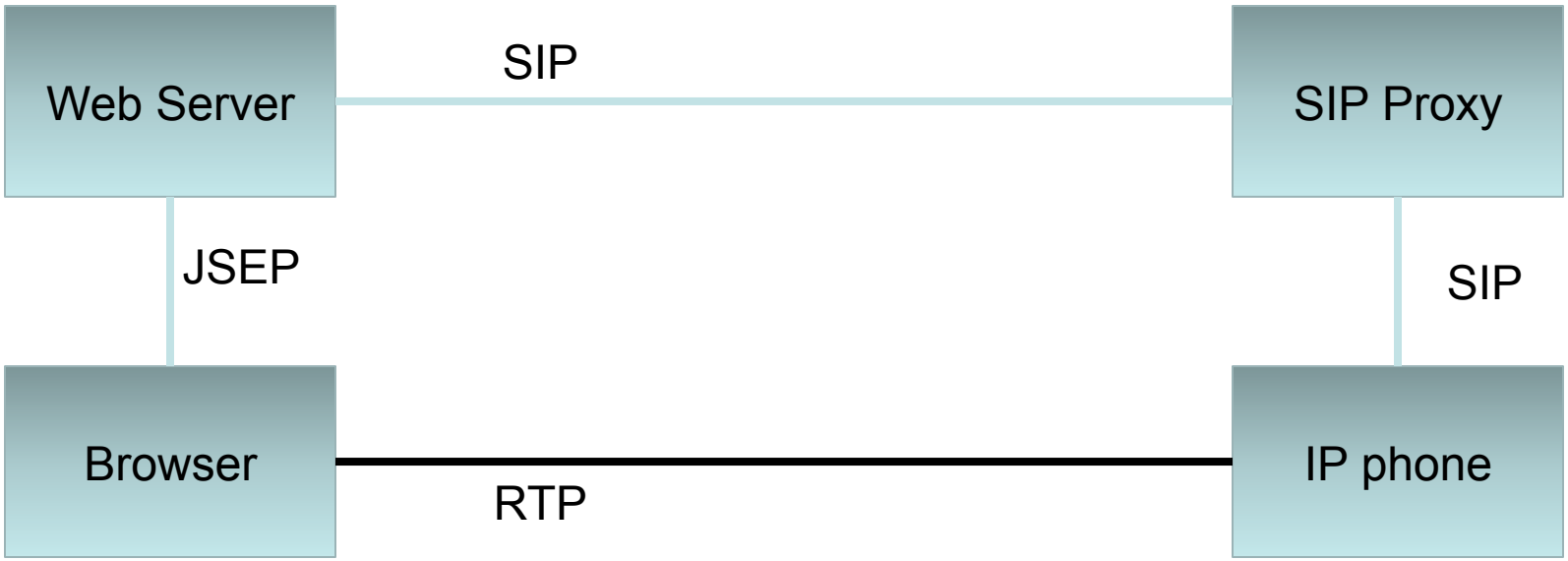
Pros

- Interoperability
- Listening by good actors
  - Debugging during development and deployment
  - Listen for faults (e.g., echo)
- Modification by good actors
  - Remove echo
  - Transcoding

Cons

- Listening by attackers
- Modification by attackers
- Identity is difficult-to-impossible

RTP Interoperability



But IP phone probably doesn't do ICE. So this slide is missing a media gateway

Debugging

- RTP is easier to debug
  - But still needs a decoder (RTP is not ASCII)
- SRTP supports NULL ciphers
  - Allows un-encrypted data on the wire
  - Now looks like RTP on the wire

Protocol Complexity

- Allowing both RTP and SRTP increases complexity
  - More code, more test cases

RTP Risks

- RTP for interoperability runs risks of RTP everywhere
- RTCWEB will be deployed everywhere
  - Not solely on managed networks
  - Coffee shop, attacker upstairs collecting traffic

SRTP

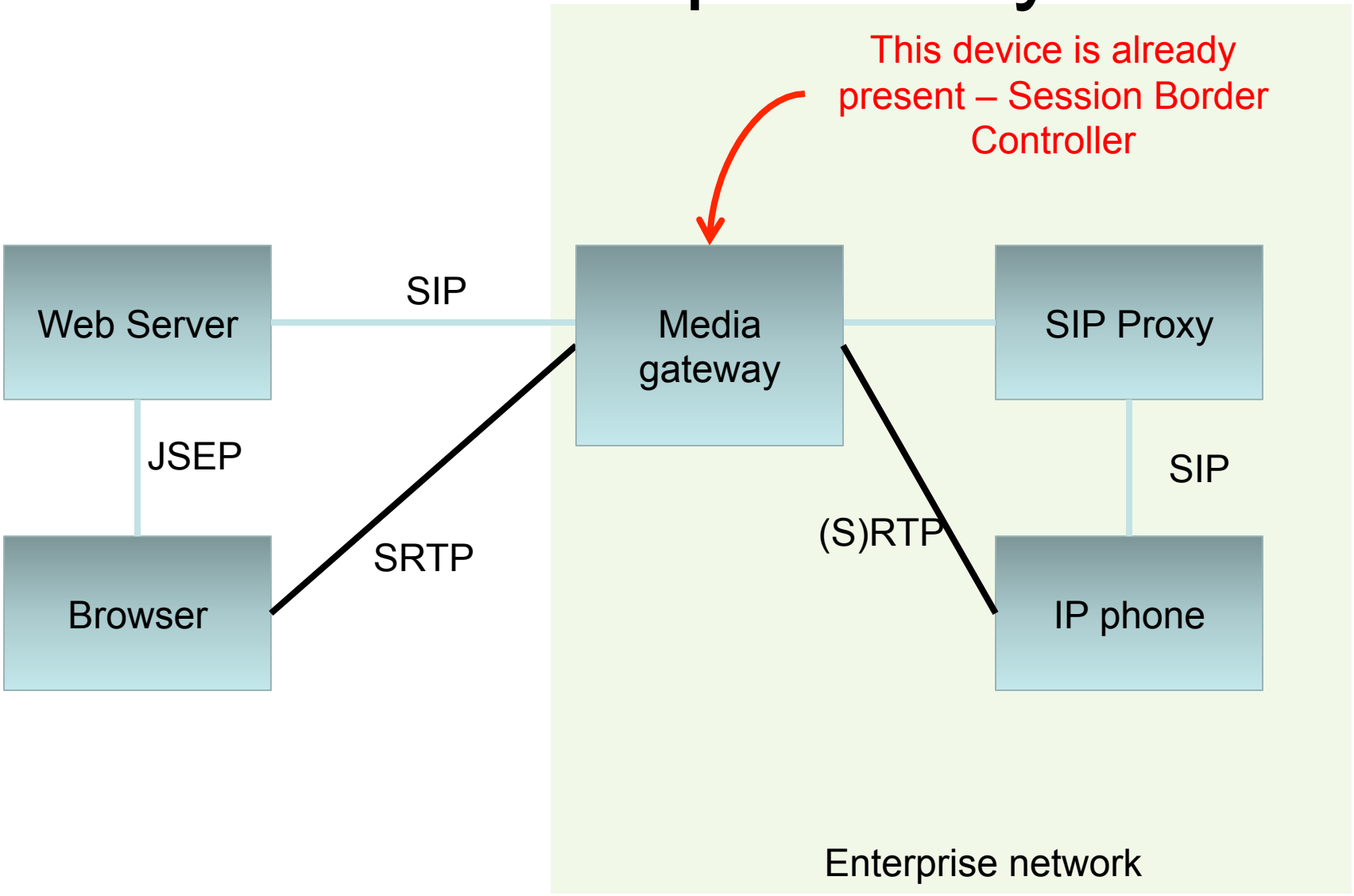
Pros

- Passive listeners need SRTP session keys
- Modification needs SRTP session keys
- Identity is possible
  - depending on keying mechanism

Cons

- We have to choose keying mechanism(s)
  - (more on that later)

SRTP Interoperability



RECORDING

Recording

- Some environments REQUIRE recording
  - jails, stock broker, bank, travel agency
- Yet need to encrypt the audio and video
  - attorney/client privilege, account number, credit card number, mother's maiden name
  - Attackers on internal network (ethernet sniffer, WiFi)
  - Attackers on the Internet
- SIPREC allows recording SRTP-encrypted flows
  - SRTP session keys are given to recorder

Independent Sessions

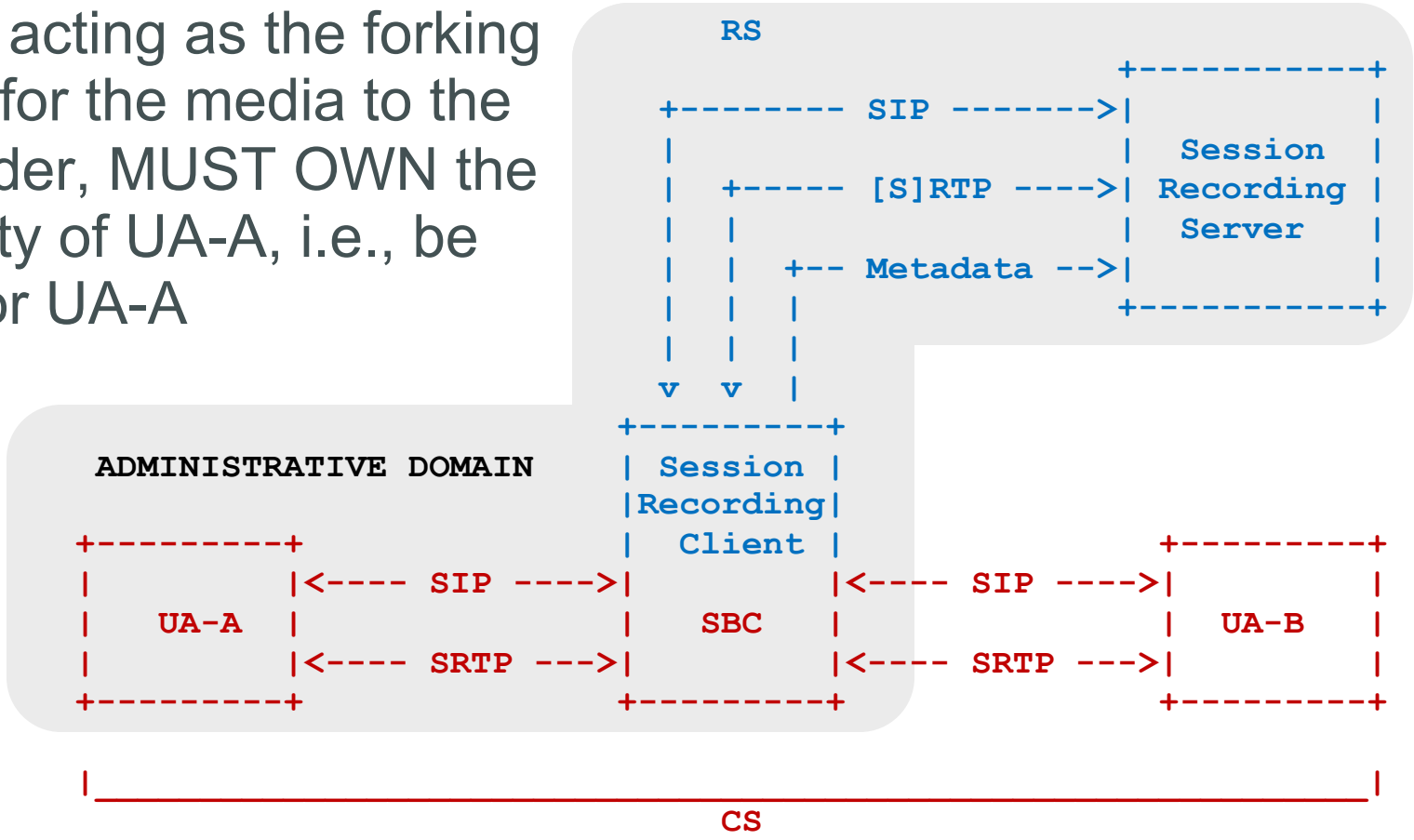
- CS = Content Session = Existing session to be recorded
- RS = Recording Session = Session established with the recorder

- Security requirements of CS != those of RS

- When SRTP used in CS, decryption/re-encryption may occur in RS

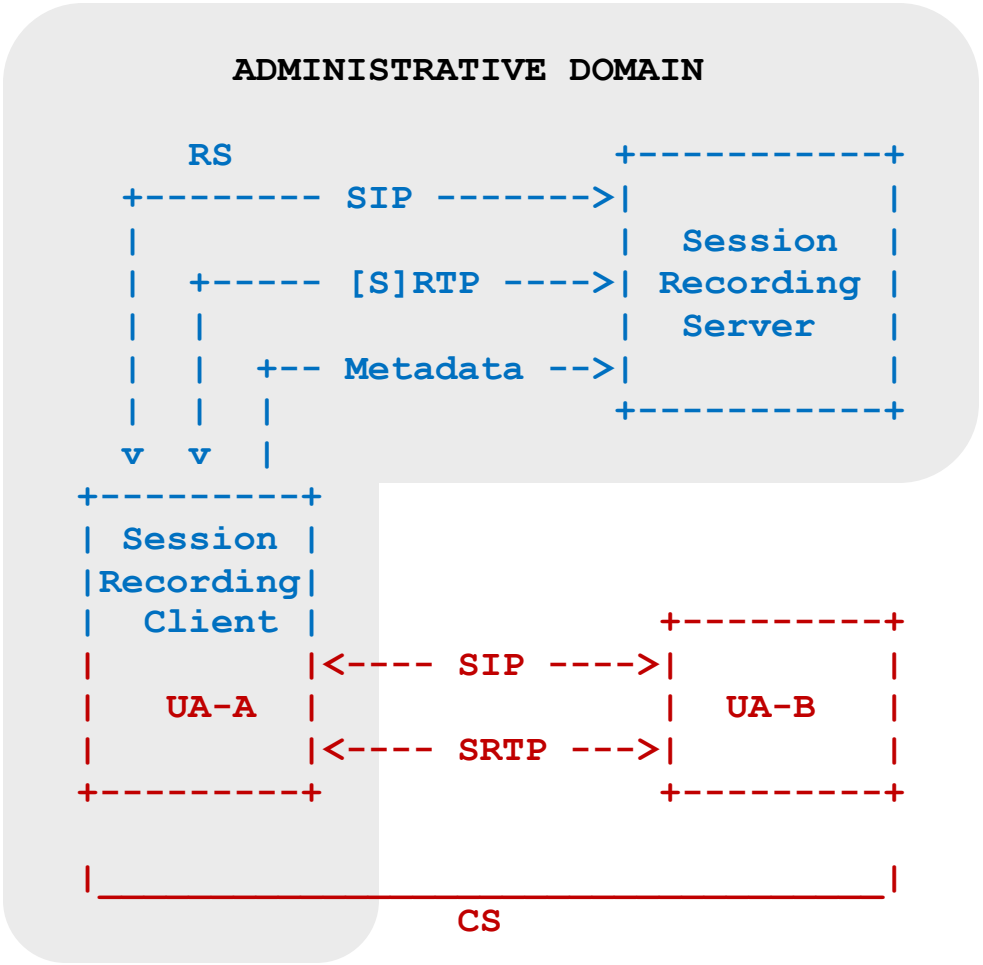
SBC Recording Model

- SBC, acting as the forking point for the media to the recorder, MUST OWN the identity of UA-A, i.e., be IdP for UA-A



UA Recording Model

- UA-A, acting as the forking point for the media to the recorder, MUST BE TRUSTED by the recorder to faithfully deliver the media.



Question for Working Group

- 15 minutes
- Is unsecured RTP necessary?

SECURITY DESCRIPTIONS VERSUS DTLS-SRTP

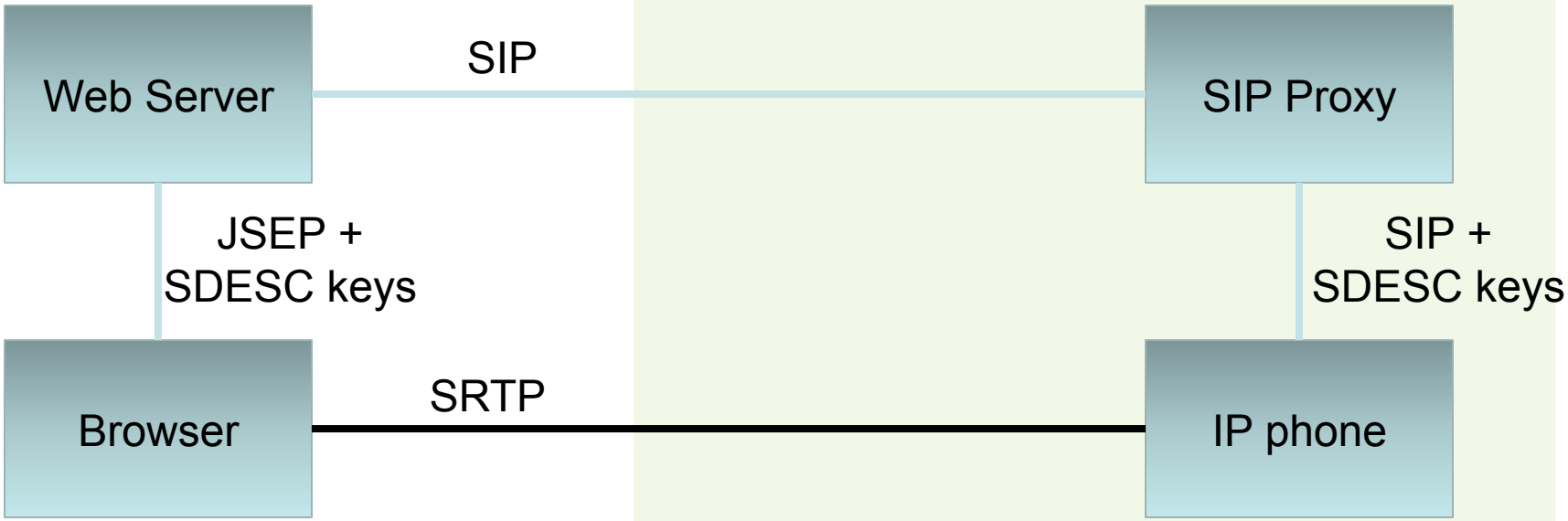
The Need for Identity

- Confidentiality is good (SDESC)
  - But not good enough
  - What if you're talking to an attacker?
- Secure communications requires peer authentication (DTLS-SRTP)
  - See EKR's plenary presentation
- User authentication comes from IdP's
  - Facebook Connect, Twitter, Google+, etc.
  - Increasingly used

Why Consider Security Descriptions at all?

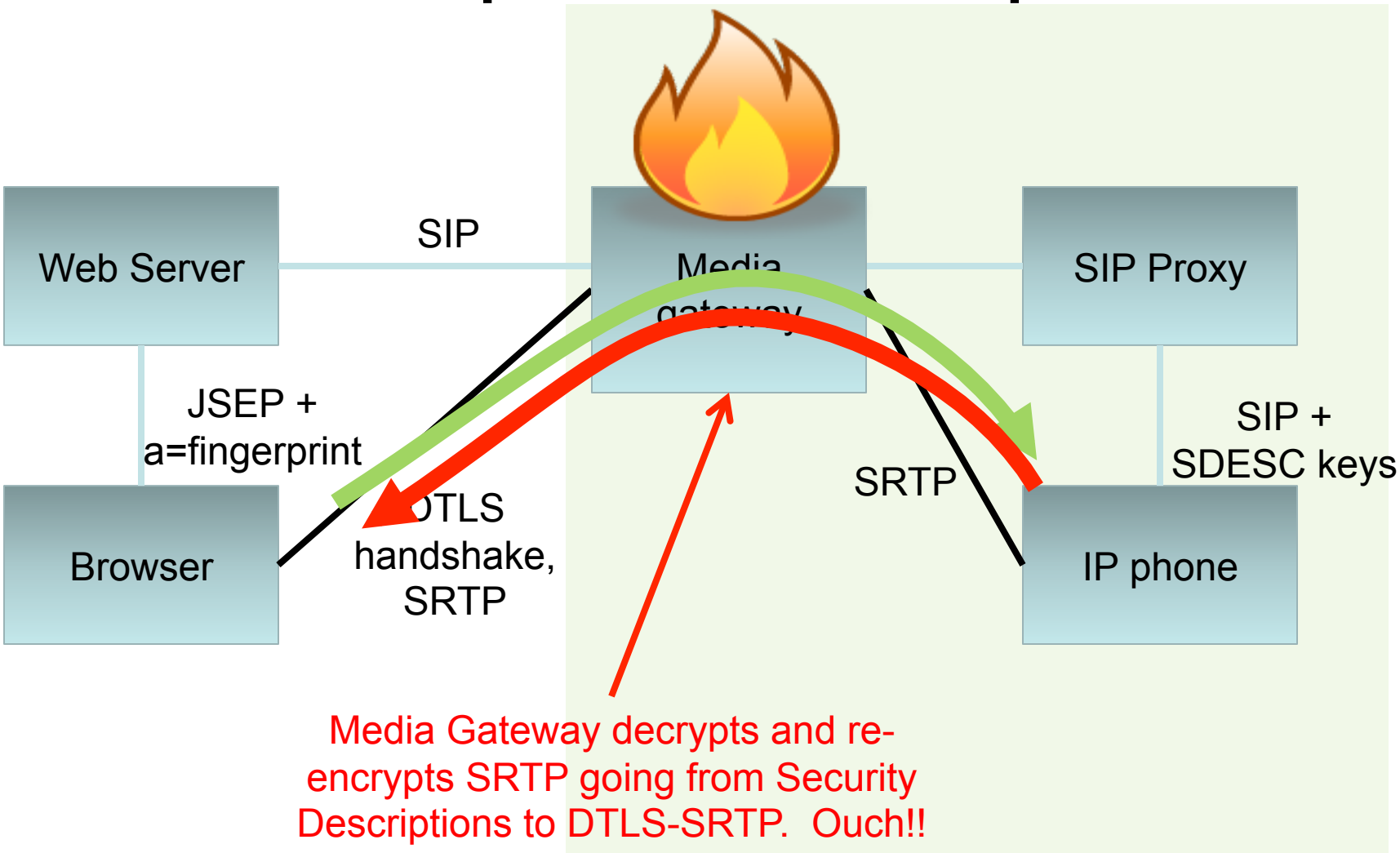
- Backwards compatibility

Security Descriptions Interop



But IP phone probably doesn't do ICE. So this slide is missing a media gateway

DTLS-SRTP and Security Descriptions Interop



Crypto Burden on Media Gateway

- Interworking DTLS-SRTP to Security Descriptions is CPU intensive
  - SRTP from DTLS-SRTP end flows easily
  - SRTP from SDESC end requires auth+decrypt, and encrypt+auth
- Reason: DTLS-SRTP handshake has both ends choose “half” of the SRTP key
- Solution: Allow each end can choose its own SRTP key, using EKT

Encrypted Key Transport (EKT)

- draft-ietf-avt-srtp-ekt-03
- Benefits:
  - Key changes share fate w/ SRTP packet itself
  - Immediate key changes (no signaling delay)
  - Useful for group keying
- Operation:
  - Encrypts the new SRTP key using another key
  - Sends this key in SRTP (or SRTCP) packet

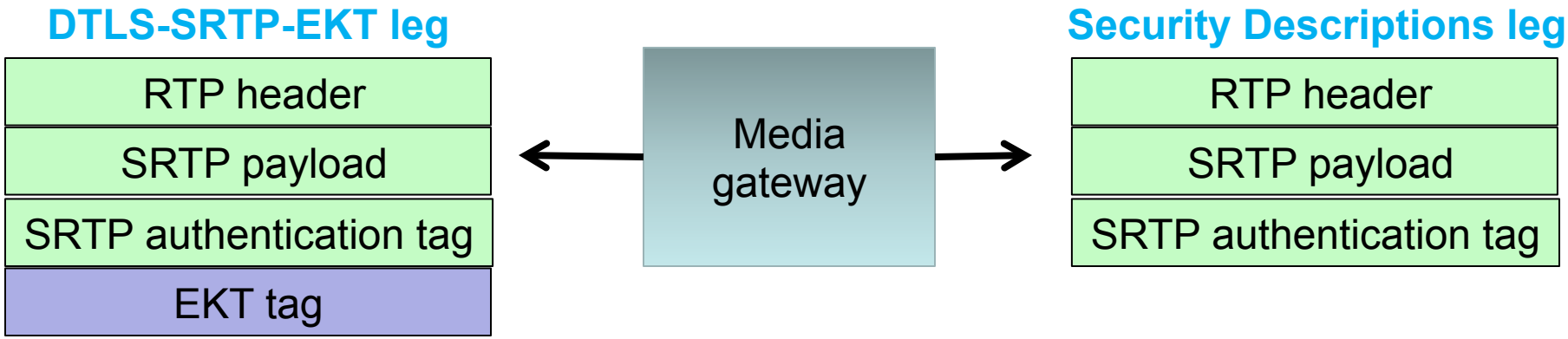
Using EKT for Interop

- Use EKT's functionality to ease interop between DTLS-SRTP and Security Descriptions
- Mechanism: Send the Security Descriptions key using EKT

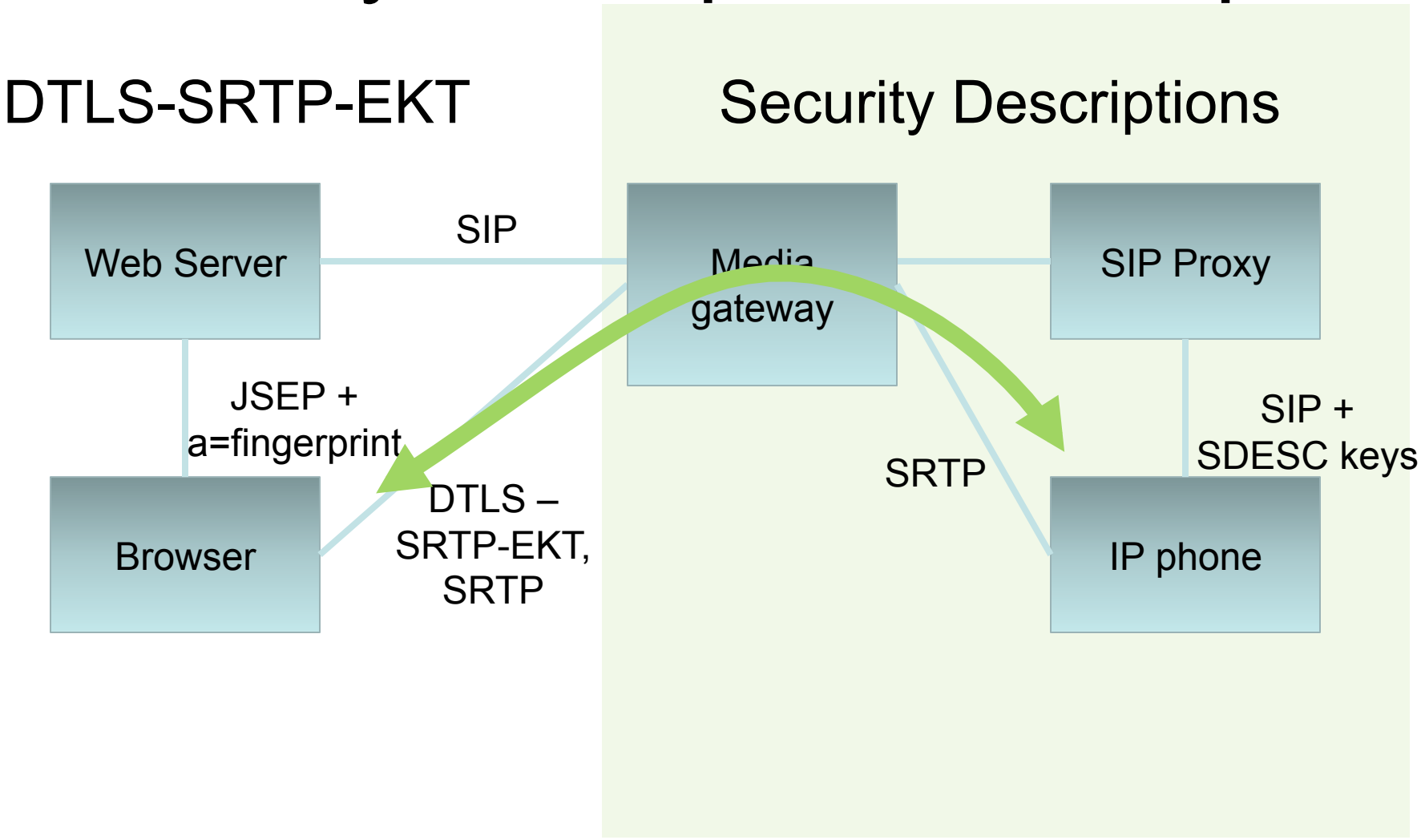
- Eliminates per-packet crypto for media gateway! Hurray!

Enhancement to EKT for Interop

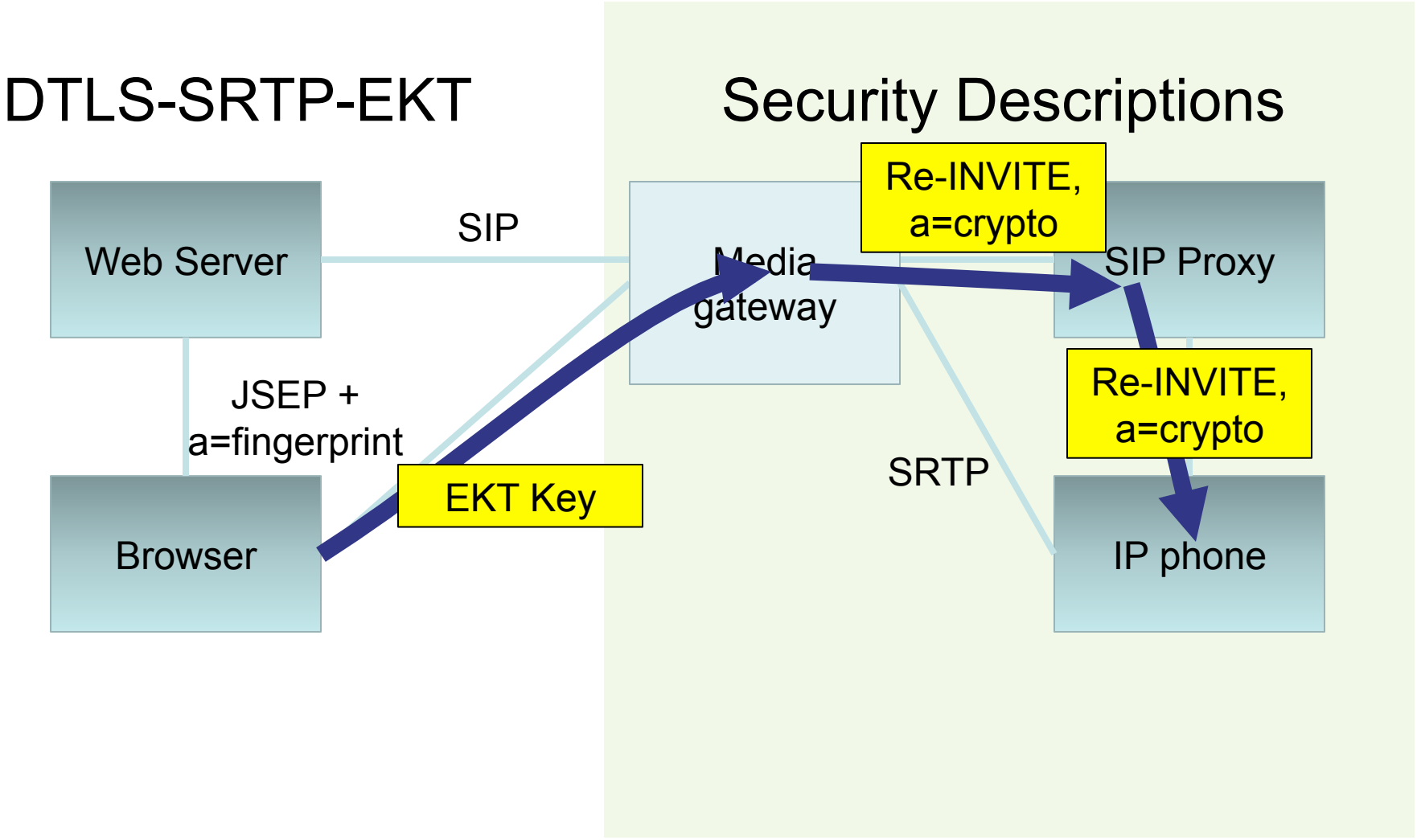
- Proposed by David McGrew on AVTCORE
- Current EKT specification replaces SRTP authentication tag with EKT tag
- Change: Retain SRTP authentication tag
- Benefit: Easy for media gateway



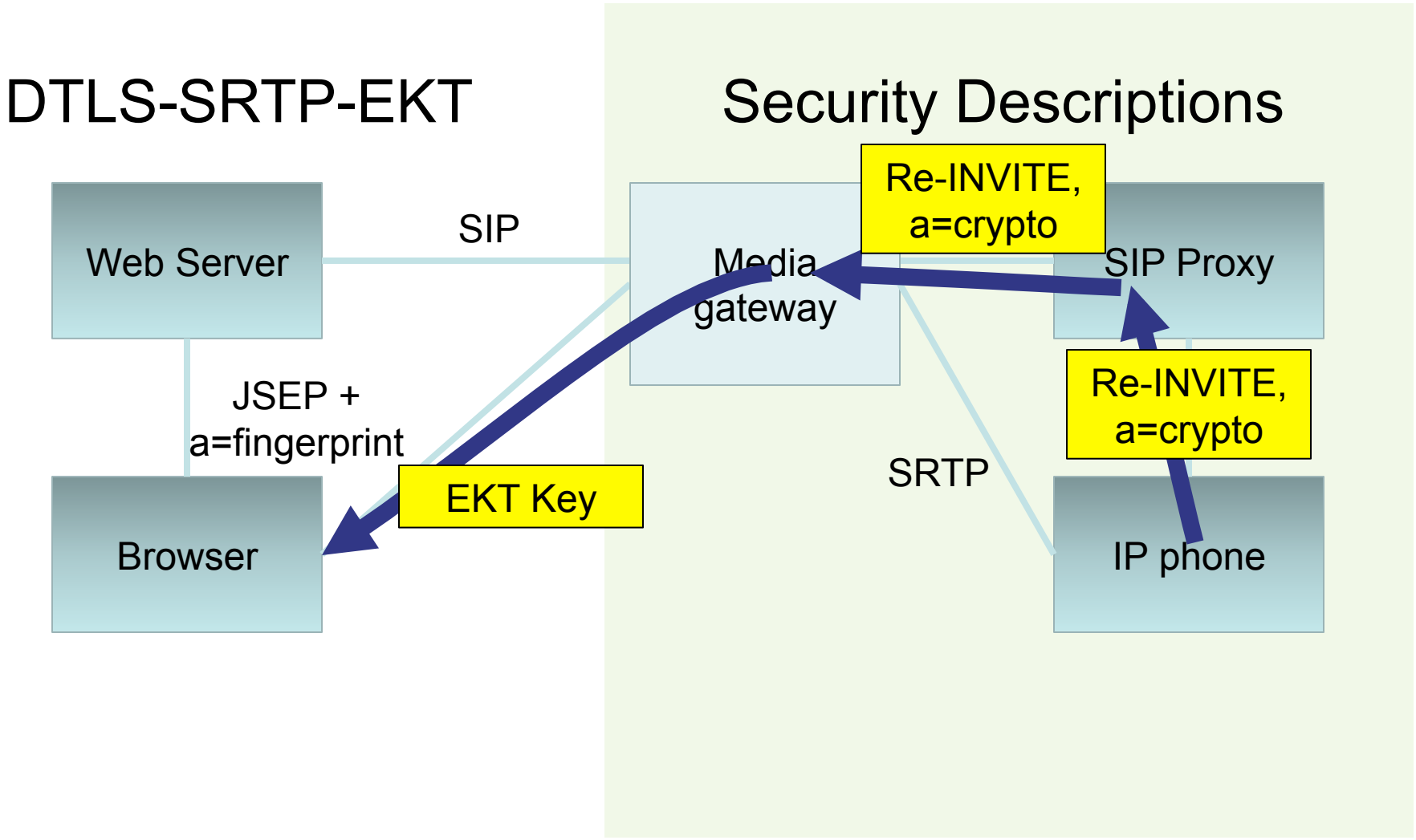
DTLS-SRTP-EKT and Security Descriptions Interop



SRTP Key Changes



SRTP Key Changes



Keying Comparison: DTLS-SRTP and SDESC

- Two RTPSEC BoFs
  - Analyzed 15 keying mechanisms
  - IETF66, July 2006
  - IETF68, March 2007
- Result was for DTLS-SRTP
- Documented in RFC5479

Security Descriptions

Pros

- Widely deployed
- No additional round trips

Cons

- Trust every signaling hop with SRTP keys
  - Log files
  - Compromised host
  - Perhaps this was acceptable within one administrative domain
- No forward secrecy
- **Cannot add identity**
- Insecure forking and retargeting

DTLS-SRTP-EKT

Pros

- Best security (RFC5479)
- Foundation for identity
  - Using fingerprints
  - Using IdP
- Group keying
- Fate sharing of SRTP key changes

Cons

- Additional round trips
- Little deployment of DTLS-SRTP(-EKT)
- Change to improve EKT interoperability is new

Removing Barriers to DTLS

- Make the DTLS handshake shorter
  - Use public keys instead of certificates
  - DTLS-SRTP doesn't use certs, anyway
  - draft-ietf-tls-oob-pubkey
- Do part of DTLS handshake in ICE connectivity checks
  - draft-thomson-rtcweb-ice-dtls
- DTLS session resumption?

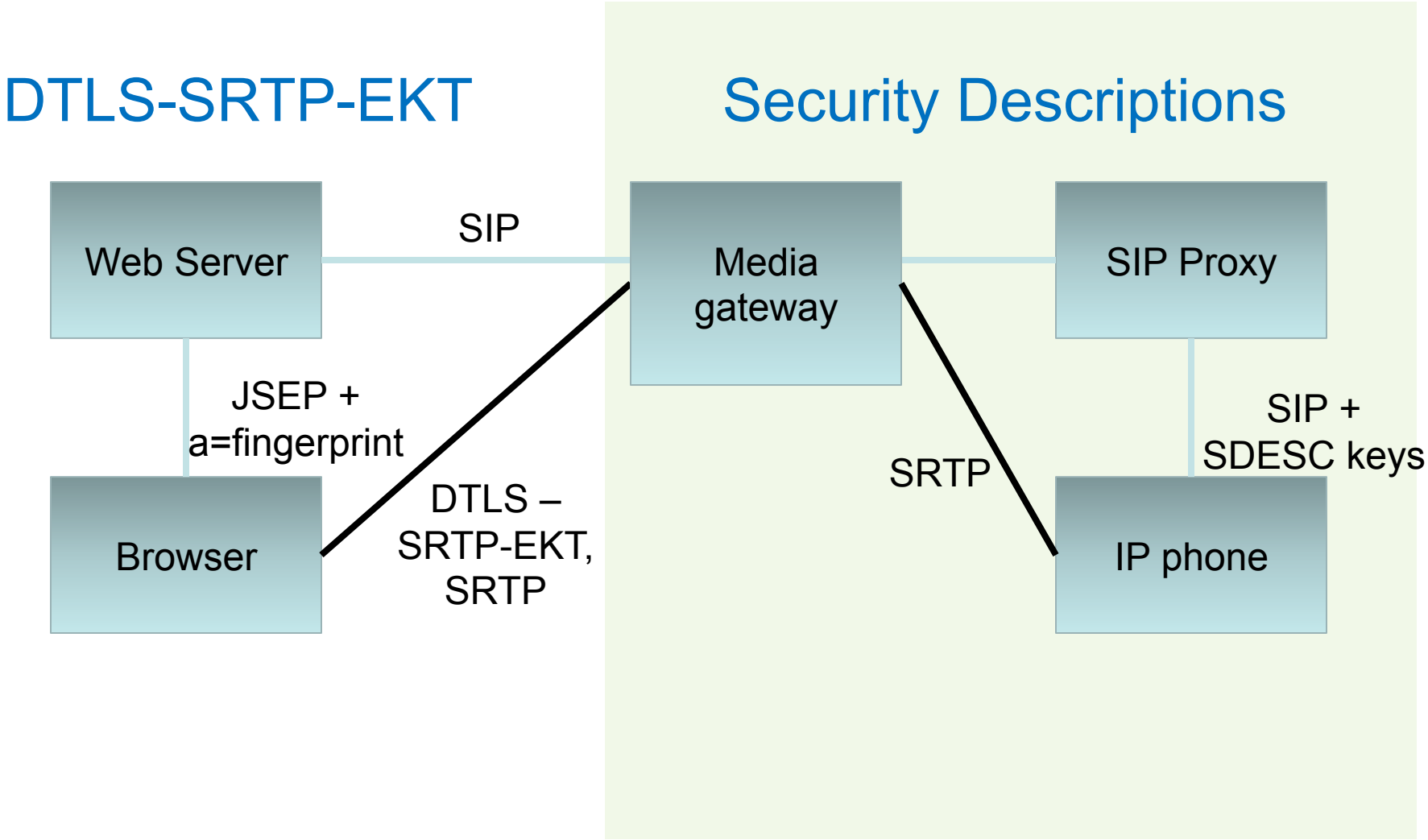
Summary of DTLS-SRTP-EKT

- Strongest security
- Allows building identity on top
- Interworks with Security Descriptions

Choices

1. DTLS-SRTP-EKT only
2. DTLS-SRTP-EKT and Security Descriptions
3. DTLS-SRTP-EKT and Security Descriptions and RTP

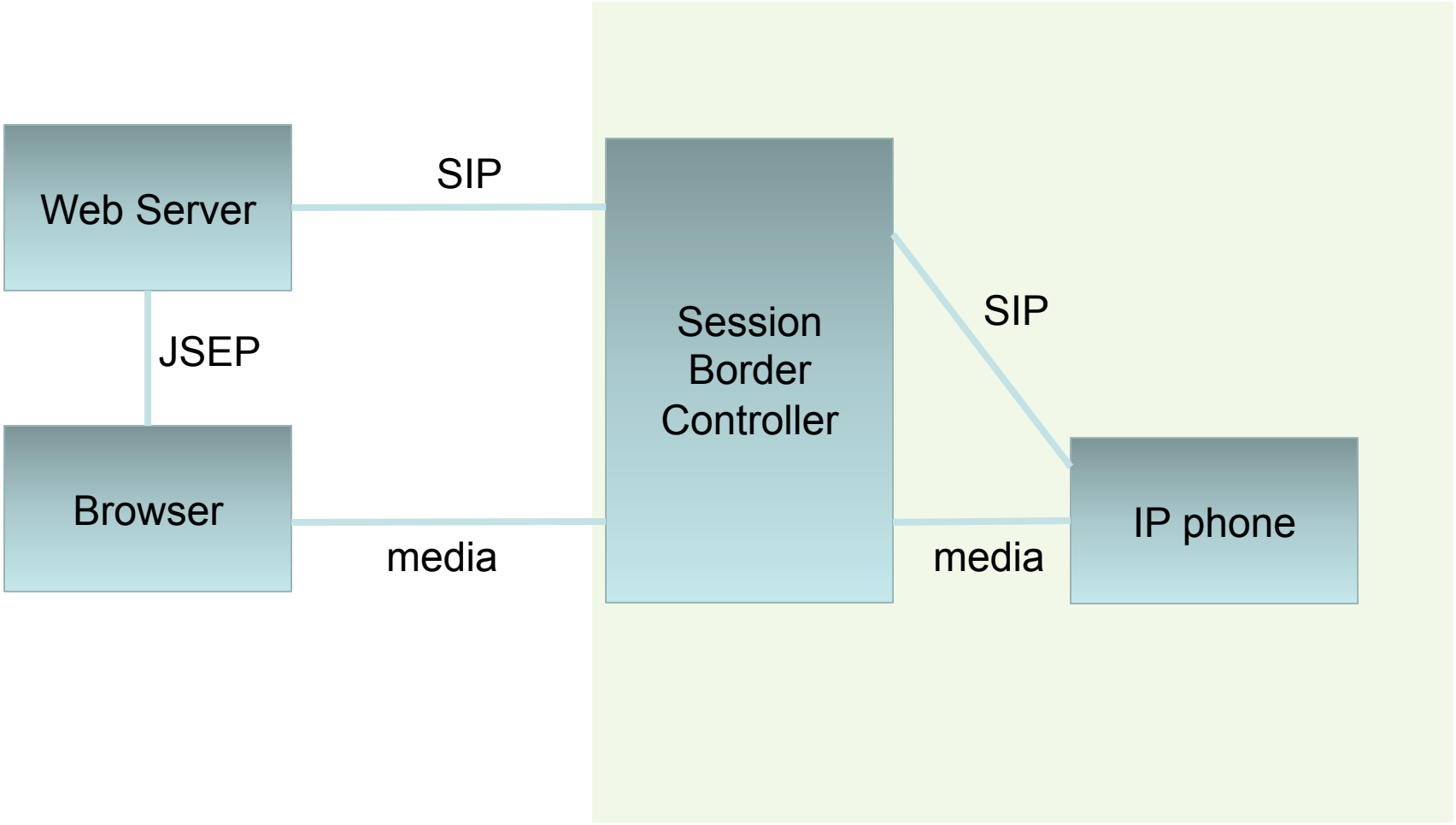
Discussion Diagram



The End

JUNK SLIDES

RTCWEB Model



Questions for Working Group

- 15 minutes