DTLS-SRTP Handling in SIP B2BUAs

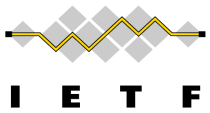
draft-ram-straw-b2bua-dtls-srtp

IETF-91

Hawaii, Nov 12, 2014

Presenter: Tirumaleswar Reddy

Authors: Ram Mohan, Tirumaleswar Reddy, Gonzalo Salgueiro, Victor Pascual



Agenda

B2BUA modes and possible MITM attacks

B2BUA Modes

1. **Media Relay**
2. Media Aware
3. Media Terminator

Legitimate Media Relay

- **Media**
  - Forwards packets without inspection or modification
  - Only modifies the L3 and L4 headers
- **Signaling**
  - It MUST forward the received certificate fingerprint without any modifications

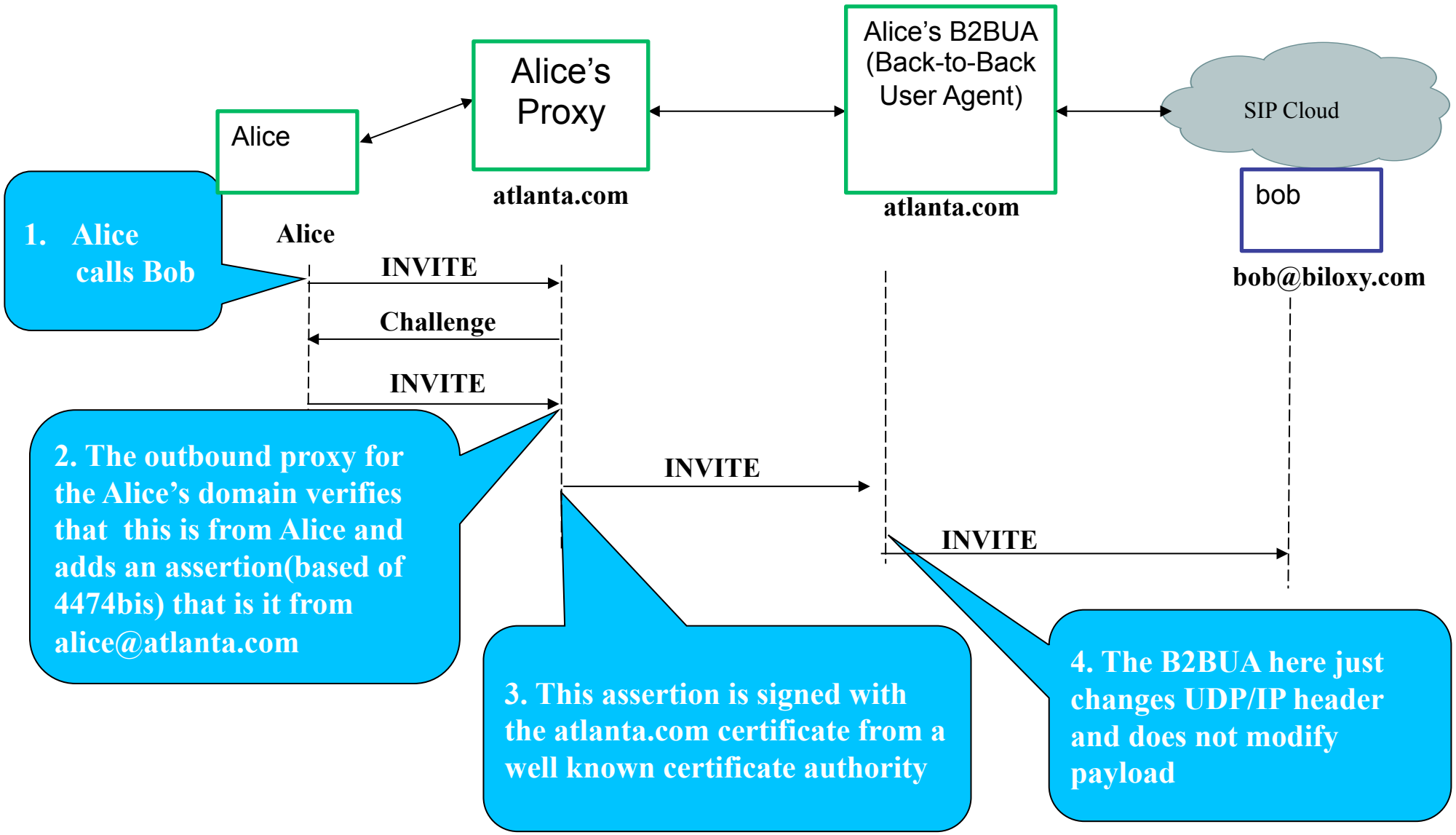
Malicious Media Relay

- **Media**
  - Forwards packets with inspection or modification
- **Signaling**
  - Modifies the certificate fingerprint and signals its own fingerprint

Possible Mitigation

- Mandate authenticated identity management in SIP (**draft-ietf-stir-rfc4474bis)**
- signed-identity-digest carries the signed hash of certificate fingerprint
- Mandate Identity headers to be present

Authenticated identity management



B2BUA Modes

1. Media Relay
2. **Media Aware**
3. Media Terminator

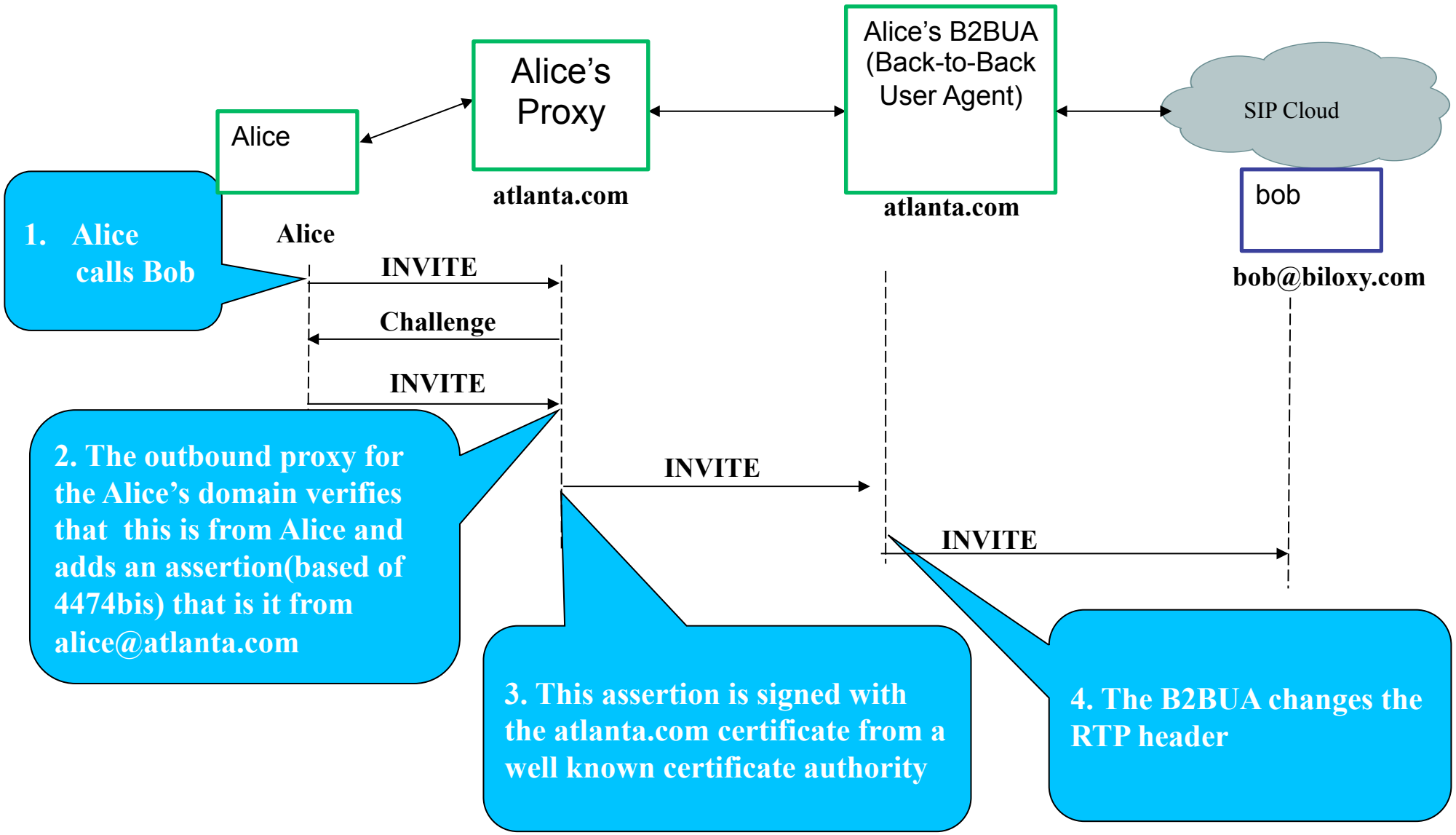
Legitimate Media Aware

- **Media**
  - Modifies the RTP header
- **Signaling**
  - Terminates the DTLS connection and acts as a DTLS proxy
    - Changes the certificate fingerprint and signals its own fingerprint
    - Decrypts and re-encrypts the payload

Malicious Media Aware

- **Media**
  - Inspects or modifies the payload.

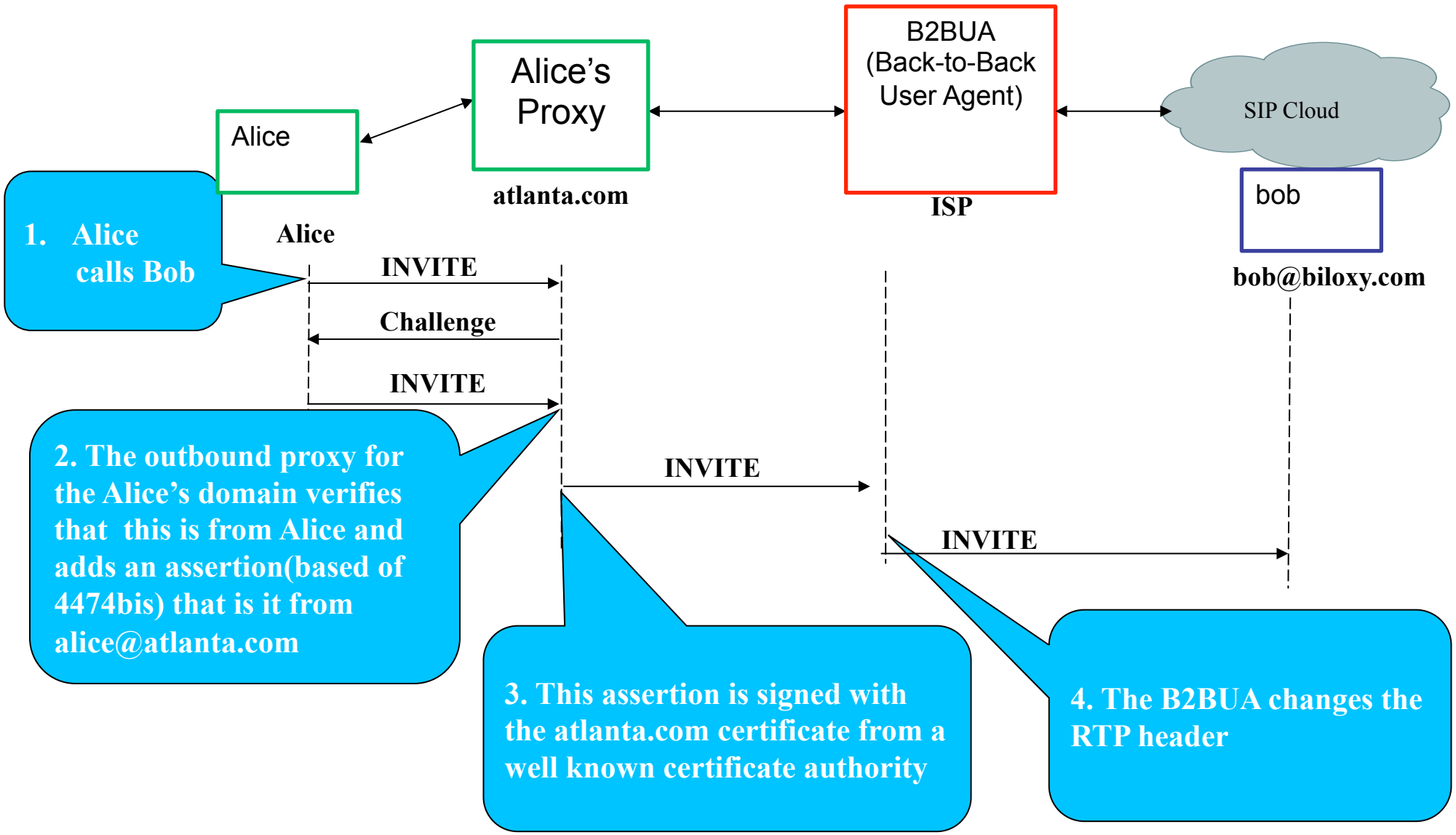
B2BUA in the same administrative domain



Possible mitigations

- Option 1> SRTP for cloud services (draft-cheng-srtp-cloud-00) proposes a mechanism where confidentiality and message authentication is independent of the RTP header
- Option 2> Trust the B2BUA

B2BUA in different administrative domain



Possible mitigation

- SRTP for cloud services (draft-cheng-srtp-cloud-00) proposes a mechanism where confidentiality and message authentication is independent of the RTP header

B2BUA Modes

1. Media Relay
2. Media Aware
3. **Media Terminator**

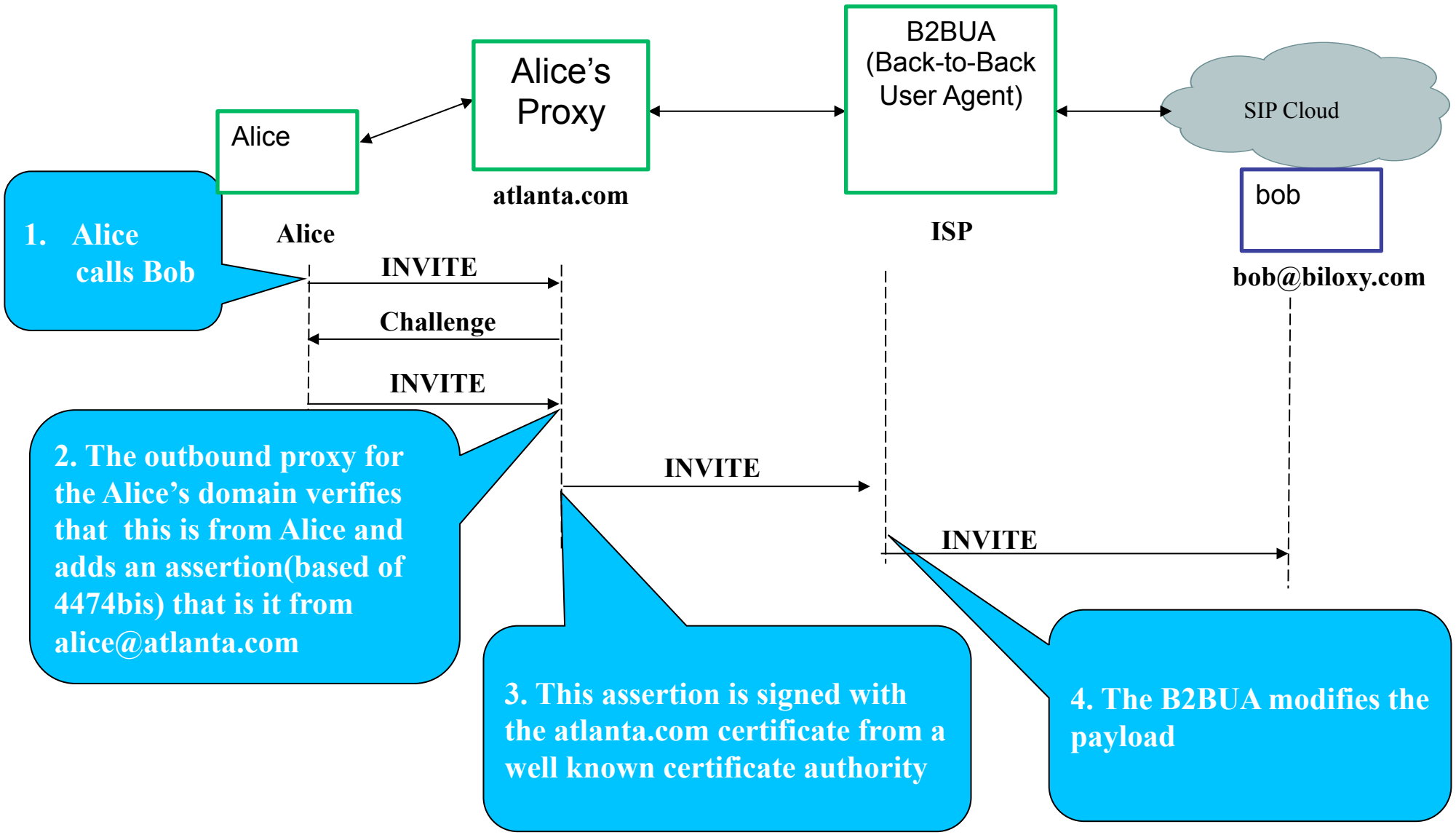
Media Terminator

- Media terminator modifies the payload
- Terminates the DTLS connection, acts as a DTLS proxy
  - Changes the certificate fingerprint and signals its own fingerprint
  - Decrypts and re-encrypts the payload

Possible attacks

- Breaks end-to-end security.

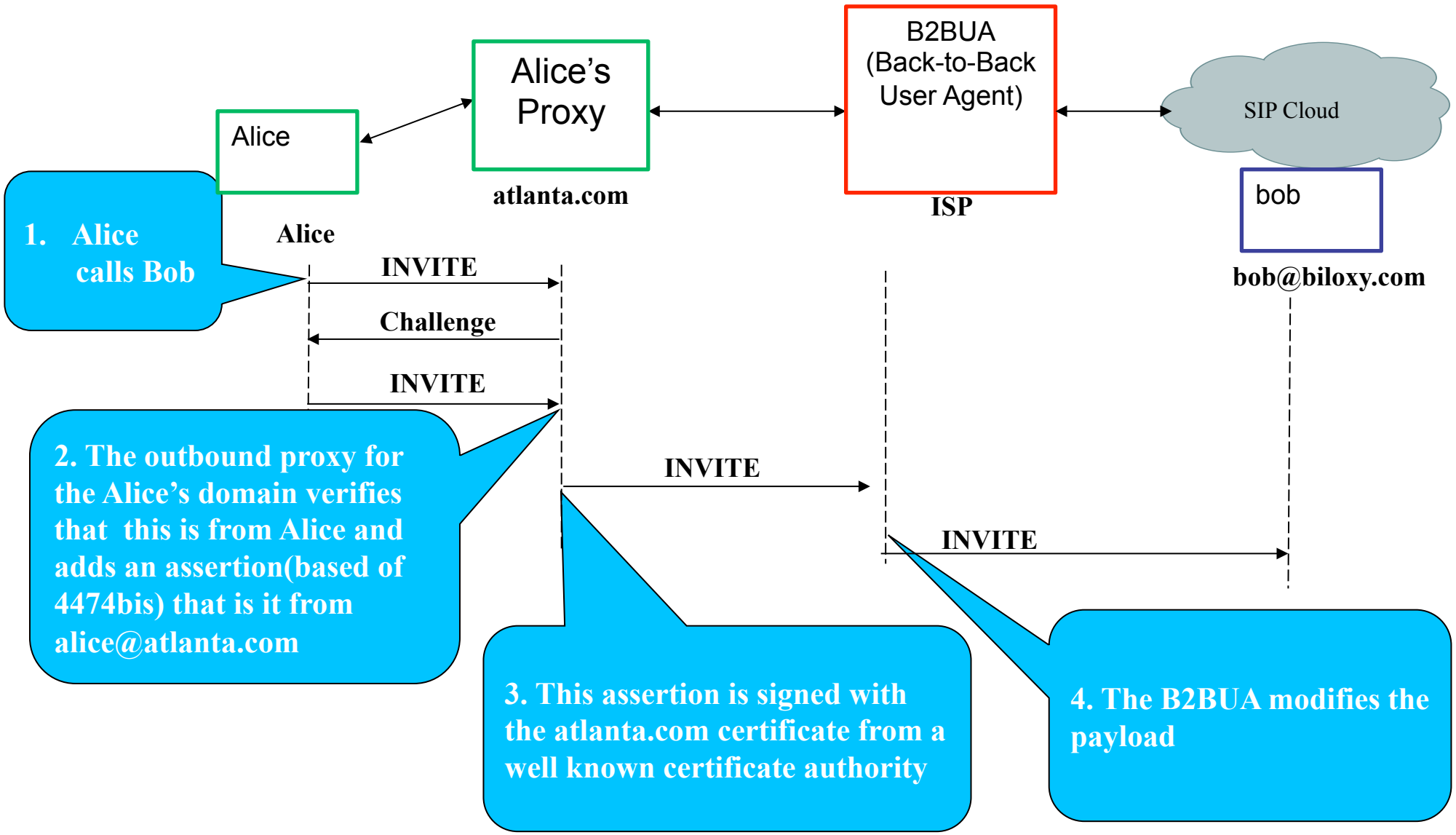
B2BUA in same administrative domain



Possible mitigations

- Clients can be configured to maintain the B2BUA server's certificate fingerprints. This way the client is aware that B2BUA is playing the role of a media-proxy.

B2BUA in different administrative domain



Possible mitigations

Discourage media terminator mode.

DTLS-SRTP Handling in SIP B2BUAs

Next Steps

Backup

B2BUA Modes

Media Relay

- Only changes UDP/IP header- e.g.: topology hiding, privacy

Media Aware

- relay which can change RTP/RTCP headers- e.g.: monitors RTCP for QoS, mux/ demuxes RTP/RTCP on same 5-tuple

Media Terminator

- Transcoders, Conference Servers