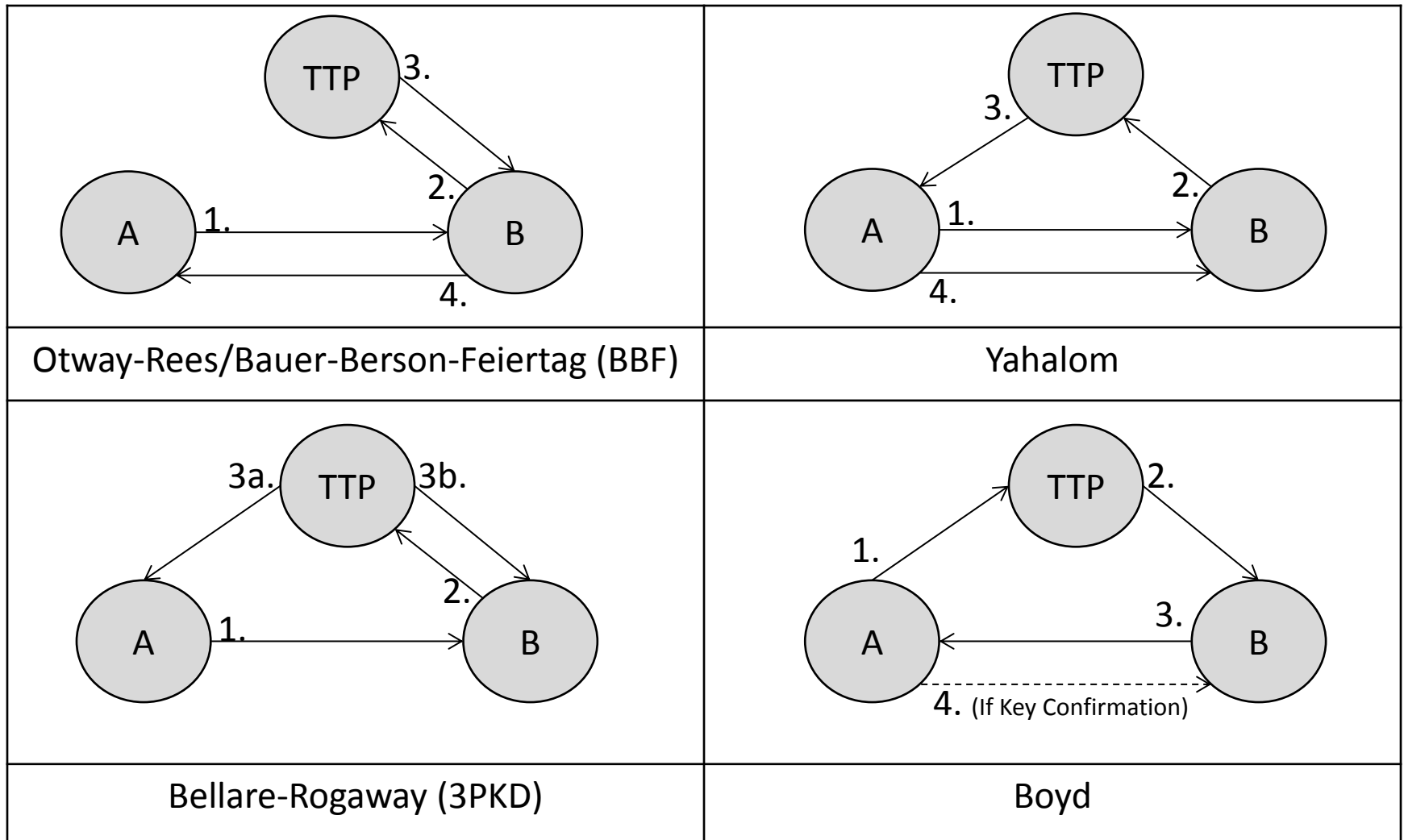


# Mapping Nonce-based 3-Party Authenticated Key Establishment Protocols

For a REST OAuth PoP-token Solution

# Nonce-based Three Party Authenticated Key Establishment (AKE)



\* At the end of the document there are links to detailed descriptions of the protocols

# Considerations

- Either RS or C can be mapped to be the sender of the first message of the AKE protocol (« A » in the Key Establishment literature)
  - We will map both alternatives for each AKE protocol (« A=C » and « A=RS »)
- In the Case of RS not having connectivity with AS the only possible solution of the studied protocols is BBF or Otway-Rees and RS acting as « A »
- On this document we focus on the flow of messages and not on the content/crypto properties.

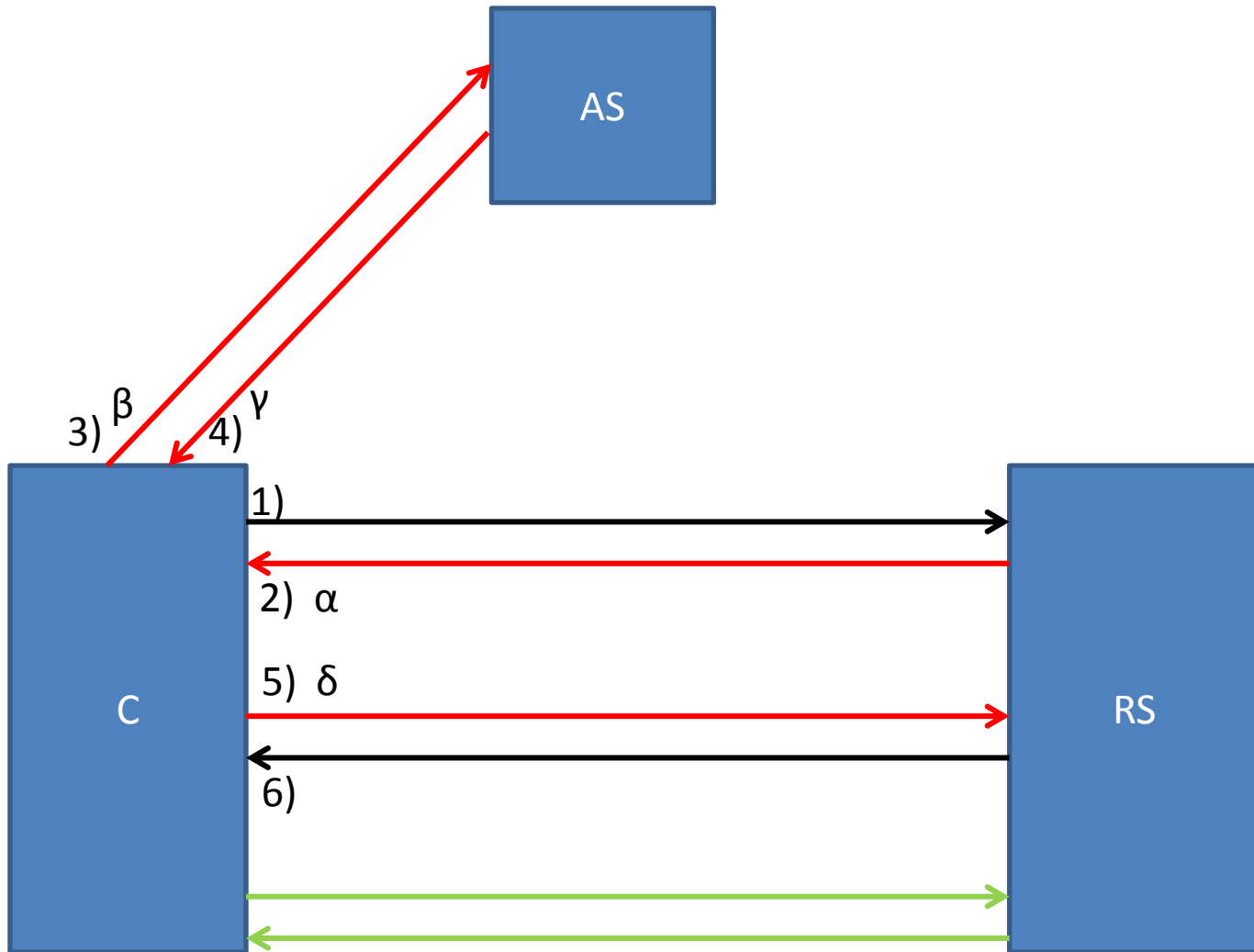
# Design Principles

- C always sends the first REST/OAuth message
- Messages are REST Request/Response Always
  - Some mappings can be improved if some REST Responses are delayed and piggyback information that in the present mappings are sent as a separate Req/Response pair of messages. No such improvements were made here.

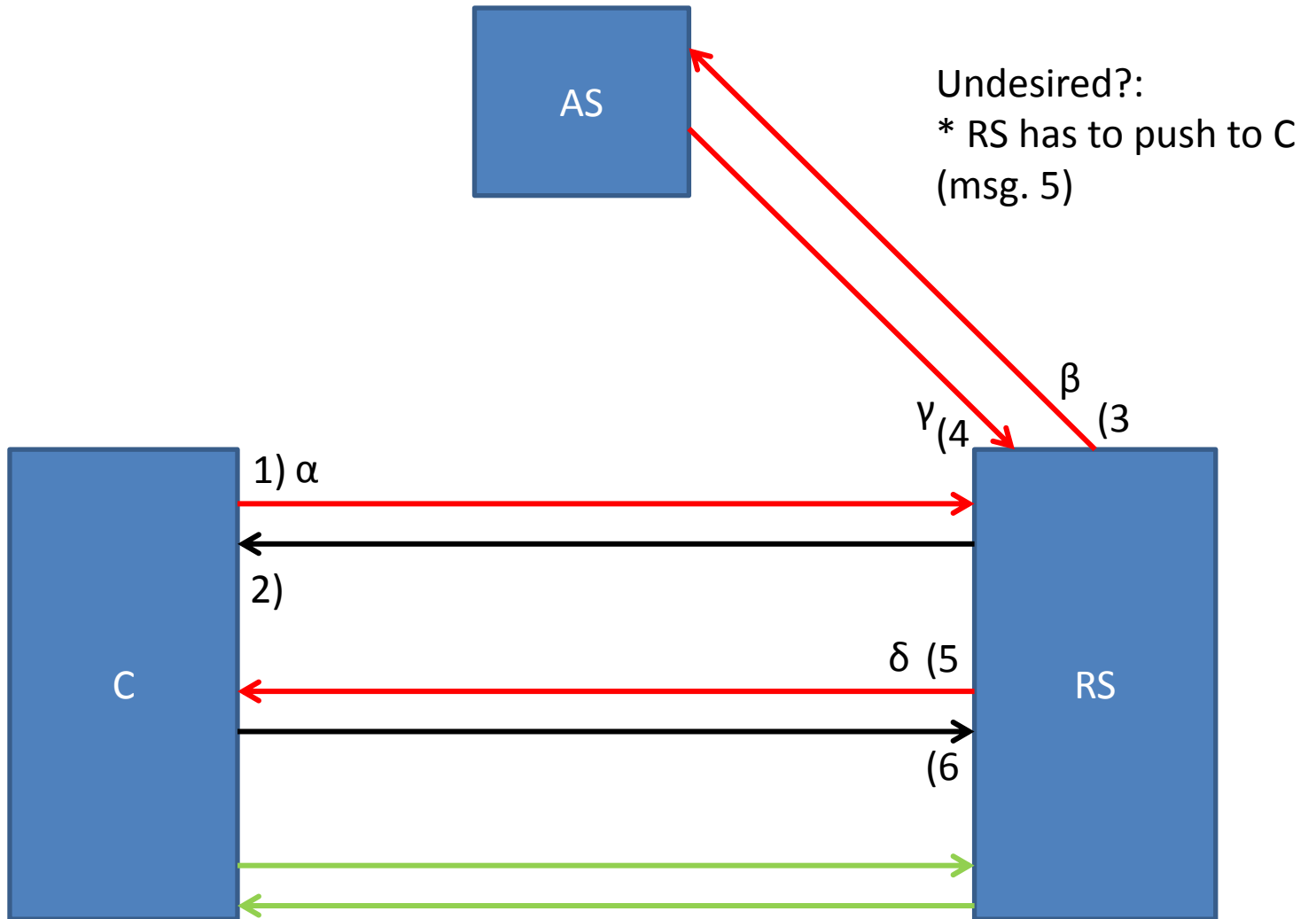
# Nomenclature/Notation

- Messages of the AKE Protocol
  - Enumeration mapped as: « 1 »  $\rightarrow \alpha$ ; « 2 »  $\rightarrow \beta$ ; « 3 »  $\rightarrow \gamma$ ; « 4 »  $\rightarrow \delta$
  - We mark the AKE protocol messages in **RED**.
- Once Protocol has finished both C and RS are in possession of the PoP-Token and the Associated fresh PSK. C can securely interact with RS. This exchange (Request and Response) is shown in **GREEN**.

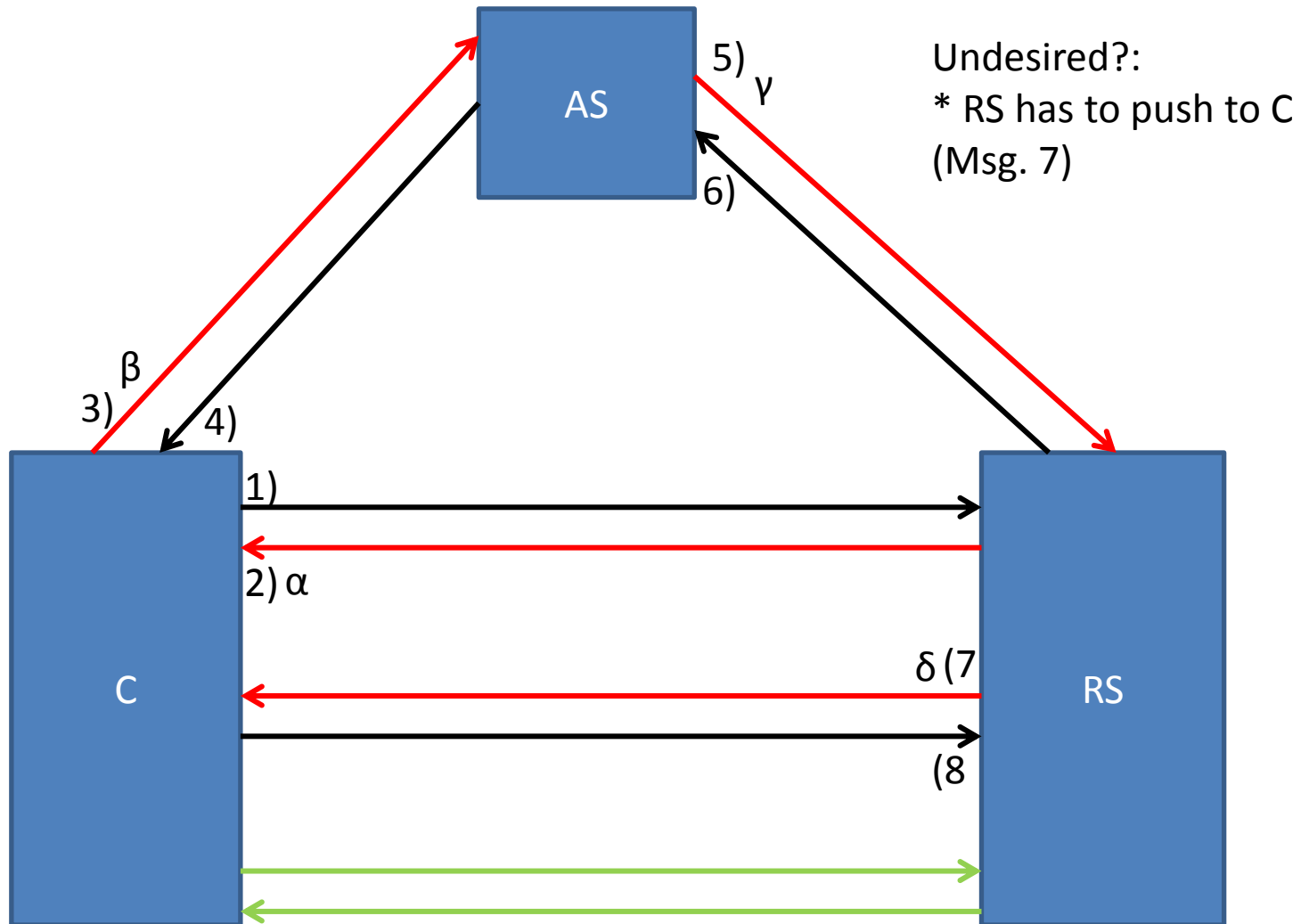
# Otway-Rees/BBF (A=RS)



# Otway-Rees/BBF (A=C)

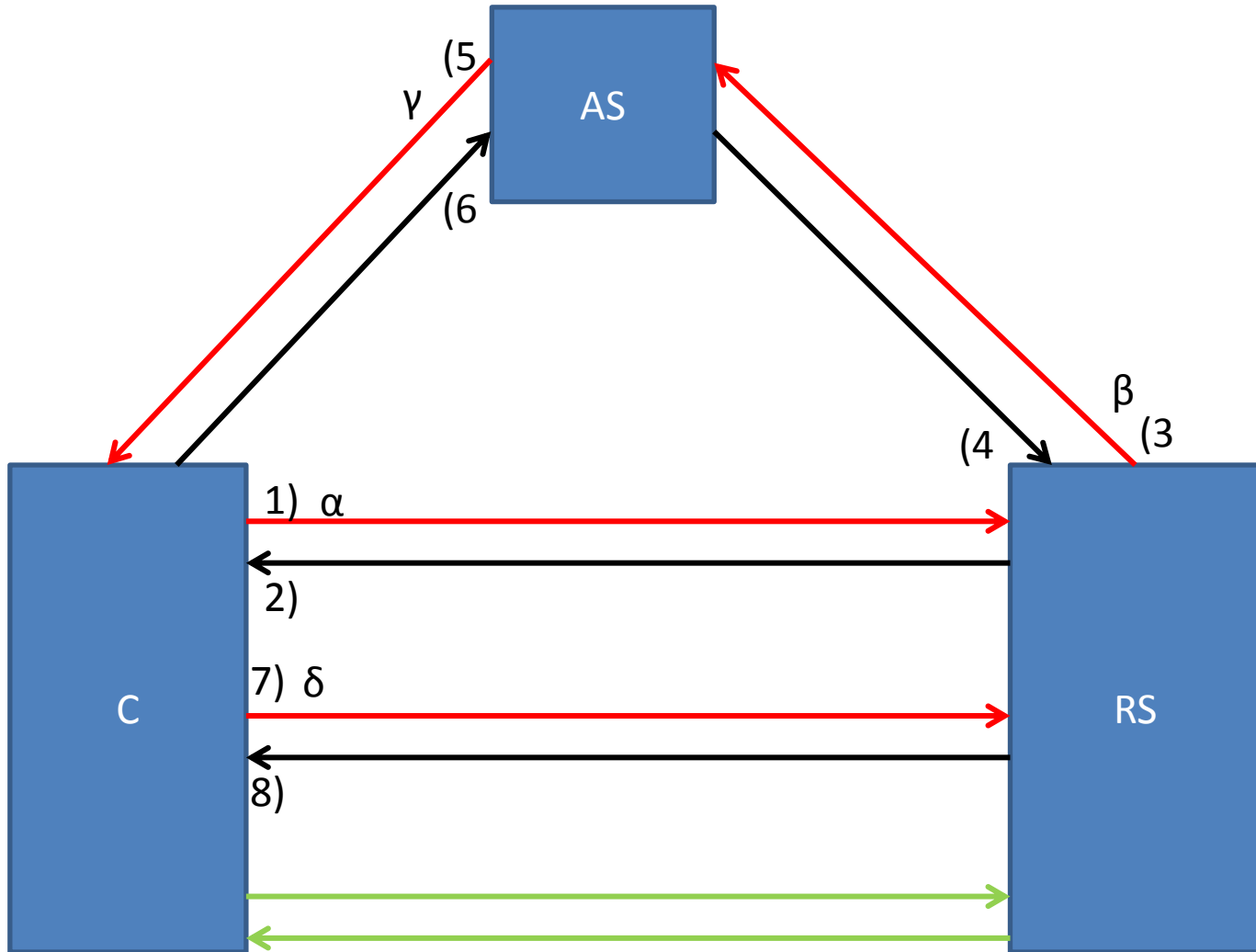


# Yahalom (A=RS)

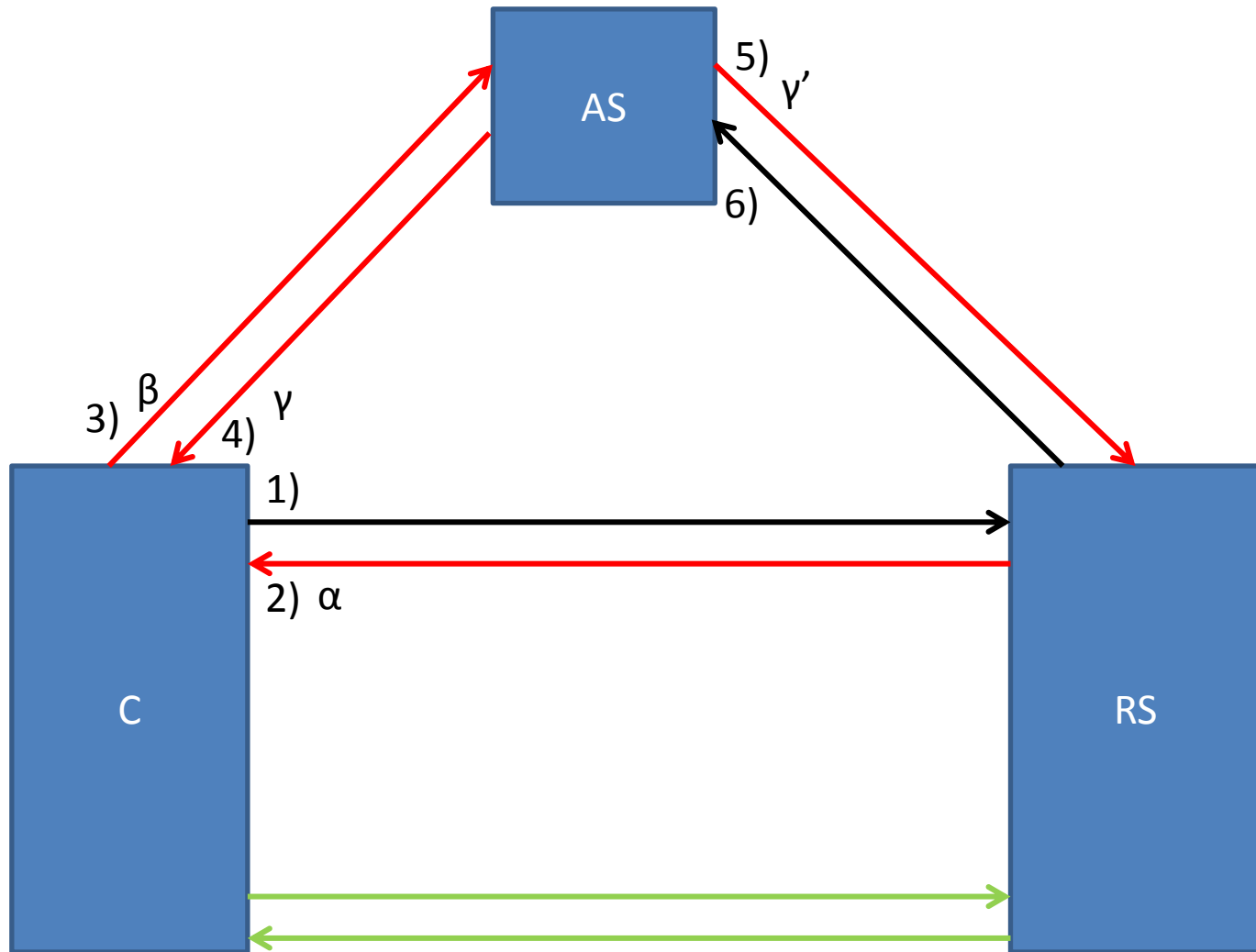




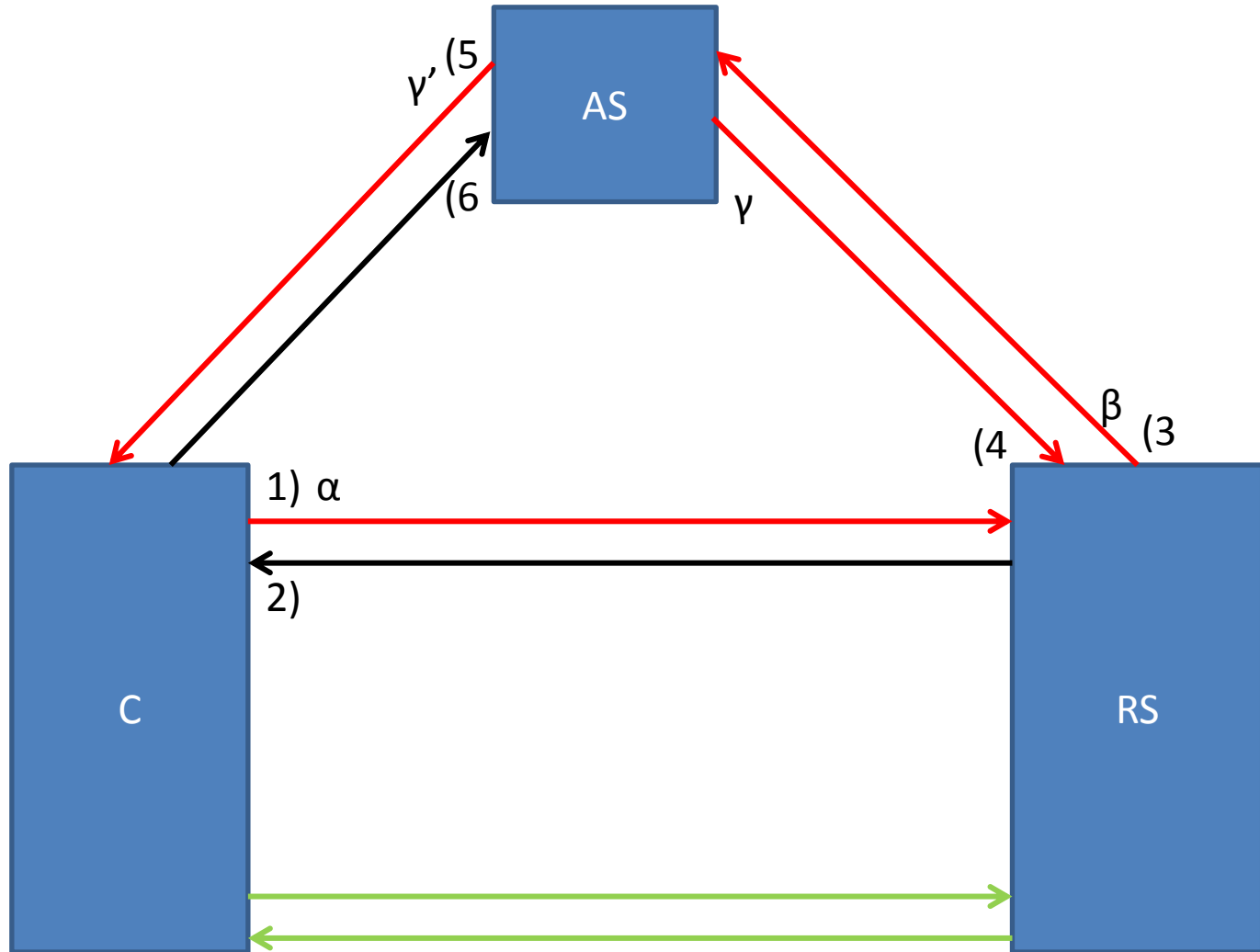
# Yahalom (A=C)



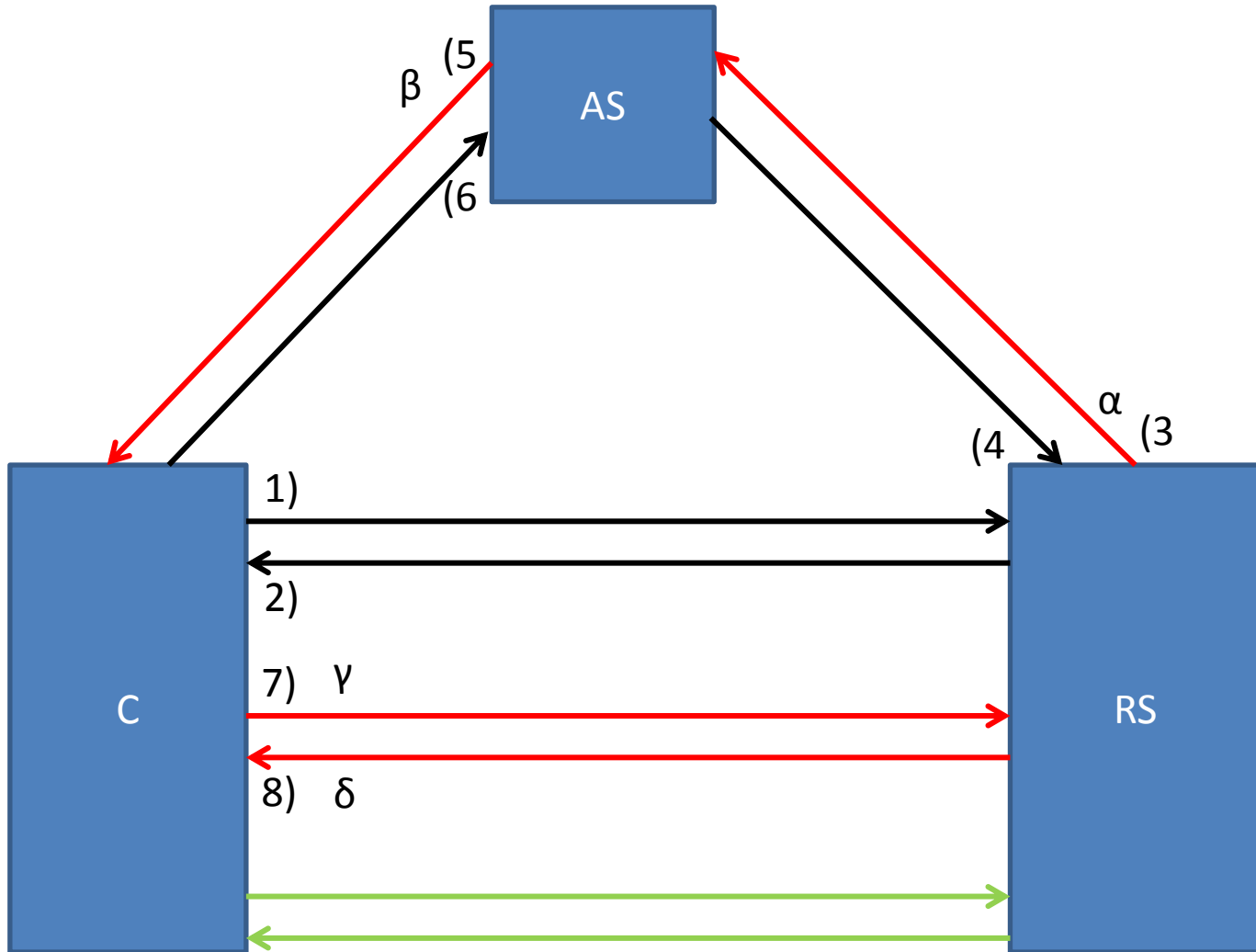
# 3PKD (A=RS)



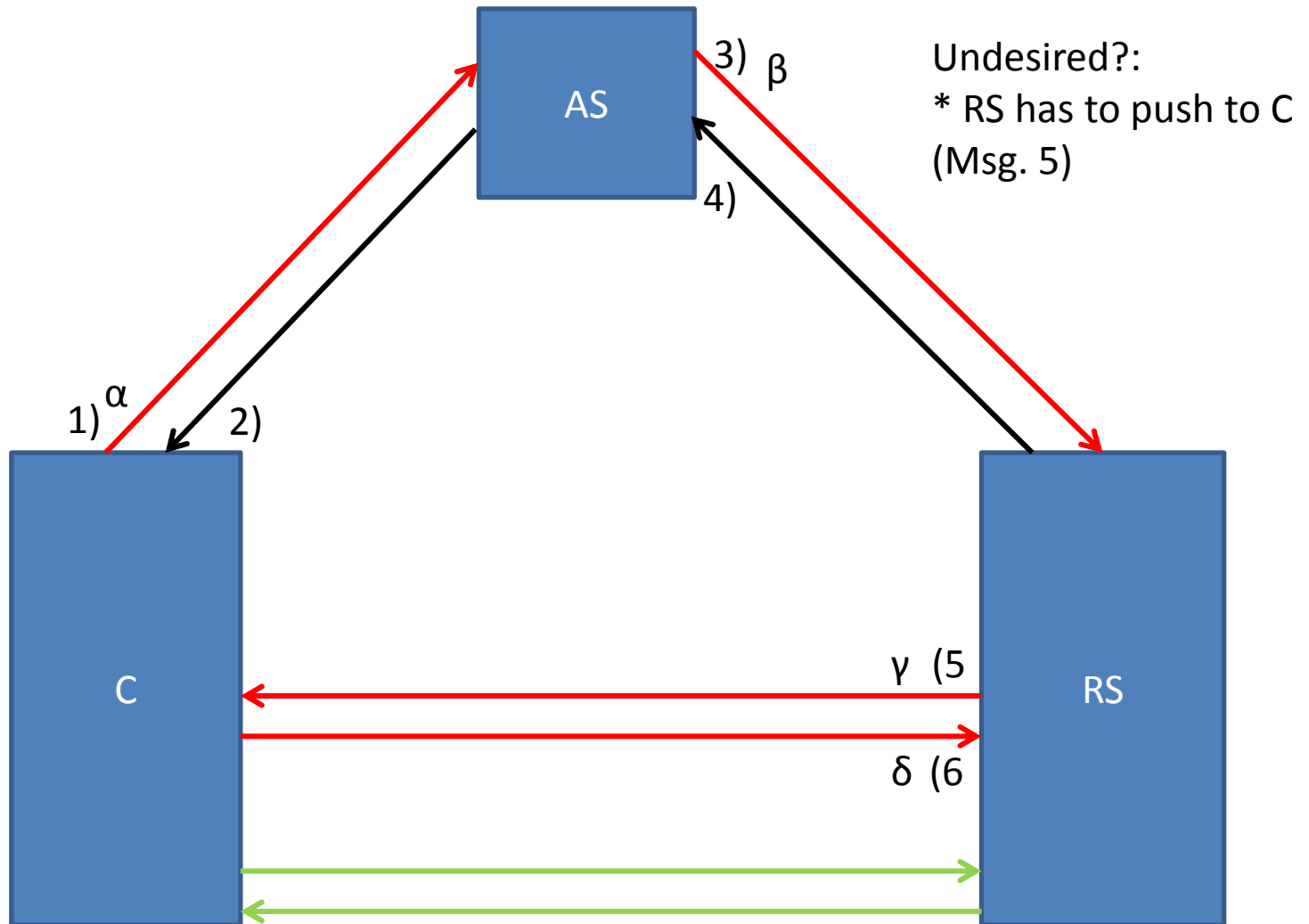
# 3PKD (A=C)



# Boyd (A=RS)



# Boyd (A=C)



# Nr. Of Messages Per Entity

	RS		C		AS		Observations
	AKE Msgs	REST Msgs	AKE Msgs	REST Msgs	AKE Msgs	REST Msgs	
Otway-Rees/BBF (A=RS)	<b>2</b>	<b>4</b>	4	6	2	2	RS directly talks only with C
Otway-Rees/BBF (A=C)	4	6	2	4	2	2	RS has to push to C
Yahalom (A=RS)	3	6	3	6	2	4	RS has to push to C
Yahalom (A=C)	3	6	3	6	2	4	
3PKD (A=RS)	<b>2</b>	<b>4</b>	3	4	3	4	
3PKD (A=C)	3	<b>4</b>	2	4	3	4	
Boyd (A=RS)	3	6	3	6	2	4	
Boyd (A=C)	3	<b>4</b>	3	4	2	4	RS has to push to C

\* We don't count the (GREEN) Messages of the Secured Req/Resp

\*\* Obs: In the RS columns we marked in **bold** the minimum values (nr msg) for each column

(If we want to minimize the msgs of RS this helps on the choice of a suitable protocol)

# AKE Protocols References

- Otway Rees :
  - <http://www.lsv.ens-cachan.fr/Software/spore/otwayRees.htm>
- Bauer-Berson-Feiertag:
  - <https://dl.acm.org/citation.cfm?id=357373> (Needs ACM Subscription)
- Yahalom:
  - <http://www.lsv.ens-cachan.fr/Software/spore/yahalom.html>
  - <https://eprint.iacr.org/2007/188.pdf> (Revised Version)
- Bellare-Rogaway (3PKD)
  - [http://eprints.qut.edu.au/1230/1/ACISP\\_Full\\_Version\\_-\\_03\\_May\\_2005.pdf](http://eprints.qut.edu.au/1230/1/ACISP_Full_Version_-_03_May_2005.pdf)
- Boyd
  - [http://eprints.qut.edu.au/4421/1/4421\\_1.pdf](http://eprints.qut.edu.au/4421/1/4421_1.pdf)