# Updating the Security BCP

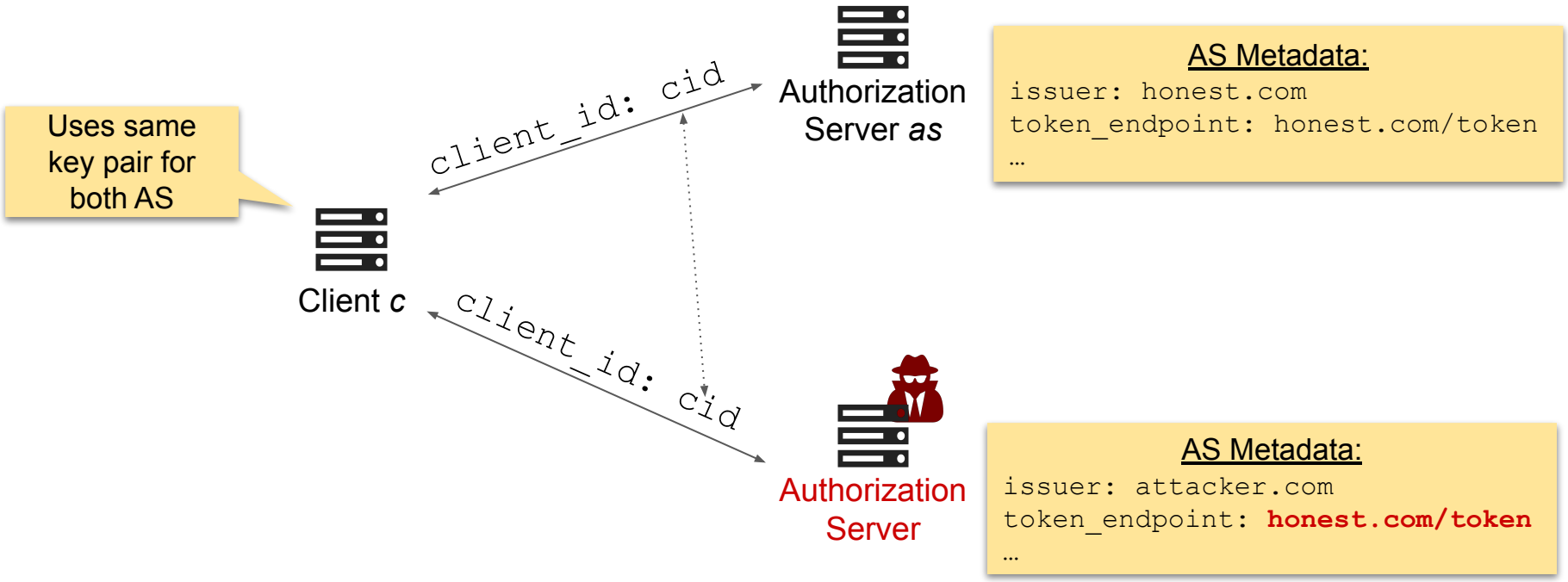
Tim Würtele
Pedram Hosseyni

University of Stuttgart, Germany

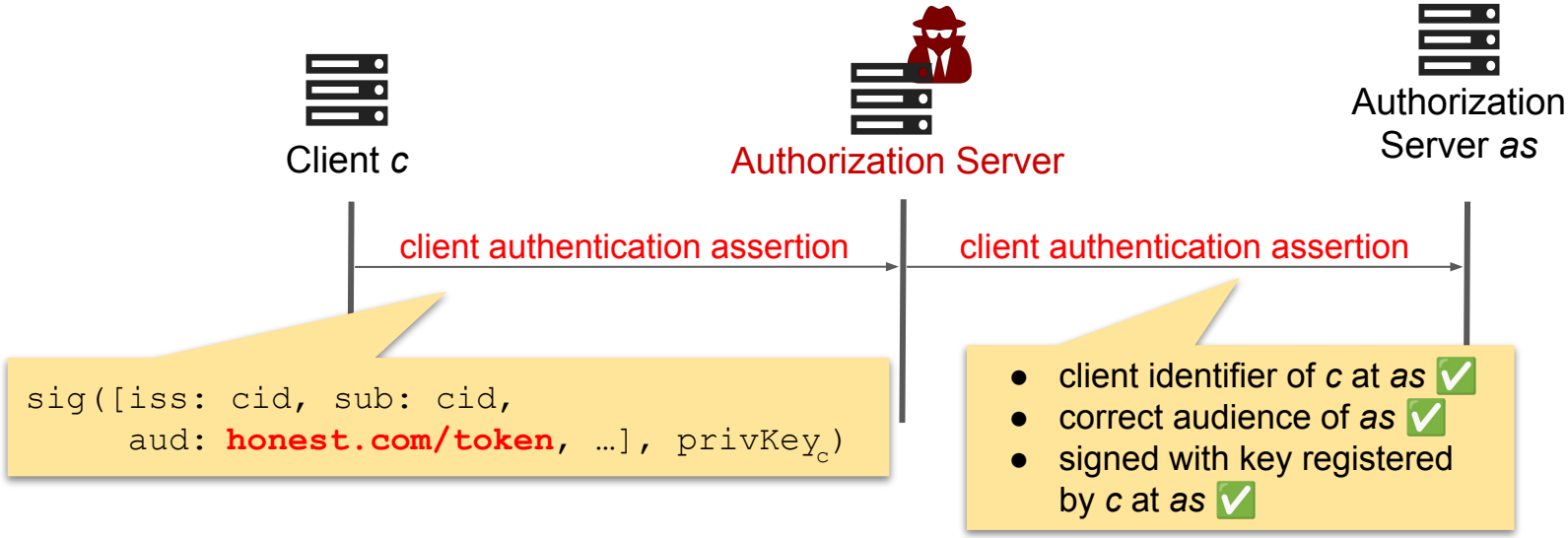
# RFC 9700 just got published … why updating it?

- Two new attacks discovered since finalization
  - Audience Injection Attacks
  - Authorization Server Mix Up Variant
- January 27: WG Interim Meeting on Audience Injection Attacks
  - Security BCP should be published now
  - Instead: Start work on an update now
  - Unrealistic to have a “finished” Security BCP

# Audience Injection Attacks (1)



# Audience Injection Attacks (2)



# Audience Injection Attacks (3)

Blog post with link to technical description:
https://openid.net/notice-of-a-security-vulnerability/

# Mix Up Reloaded

- Variant of the Mix Up already described in the BCP
- Integration Platform Context (e.g.: Google Home, Microsoft Power Automate)
- Presented during last OAuth Security Workshop by Kaixuan Luo: https://talks.secworkshop.events/osw2025/talk/WG9TEW/

# Outlook

- Any further security issues that came up recently?
  - Feel free to contact us!
    pedram.hosseyni@sec.uni-stuttgart.de | tim.wuertele@sec.uni-stuttgart.de
- Any questions or comments?