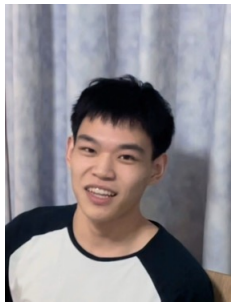
EuroS&P 2023

MISO: Legacy-compatible Privacy-preserving Single Sign-on using Trusted Execution Environments

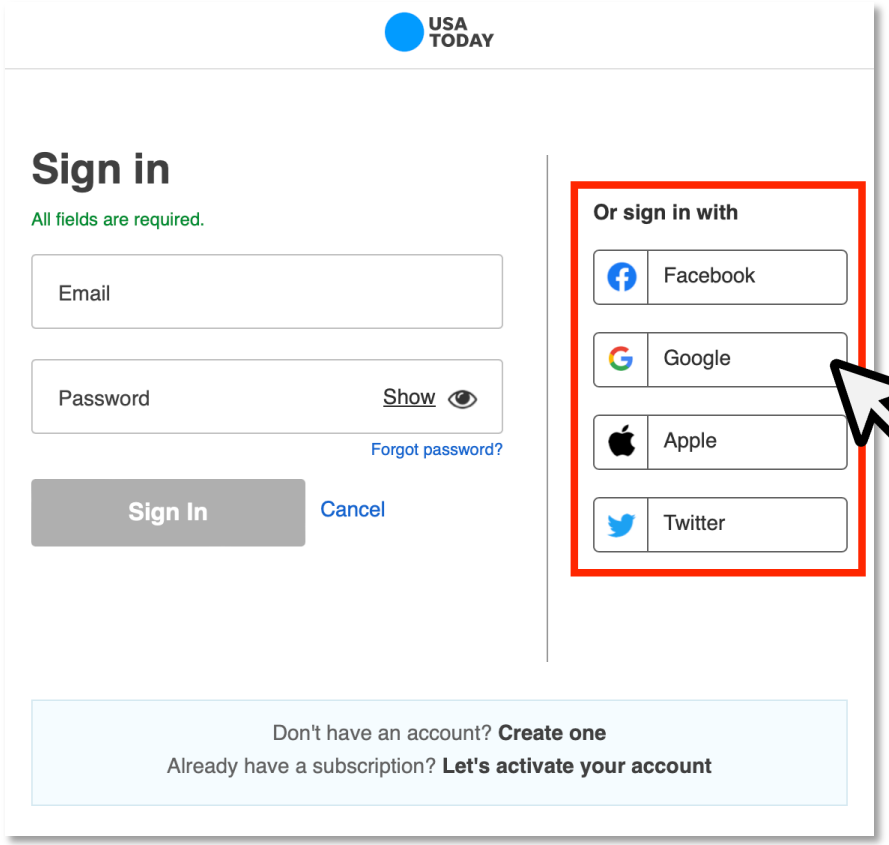
Rongwu Xu∗, Sen Yang†, Fan Zhang†, Zhixuan Fang∗

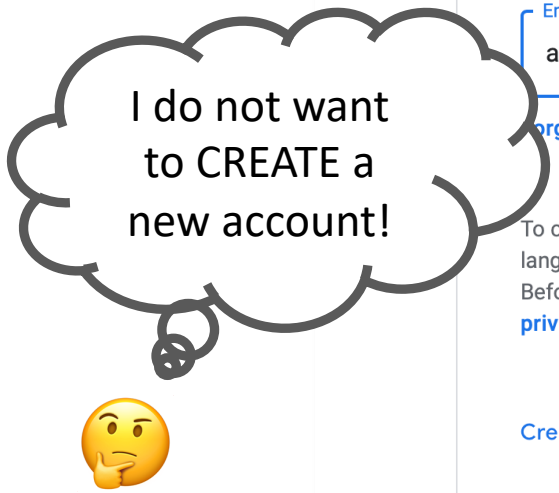
∗Tsinghua University

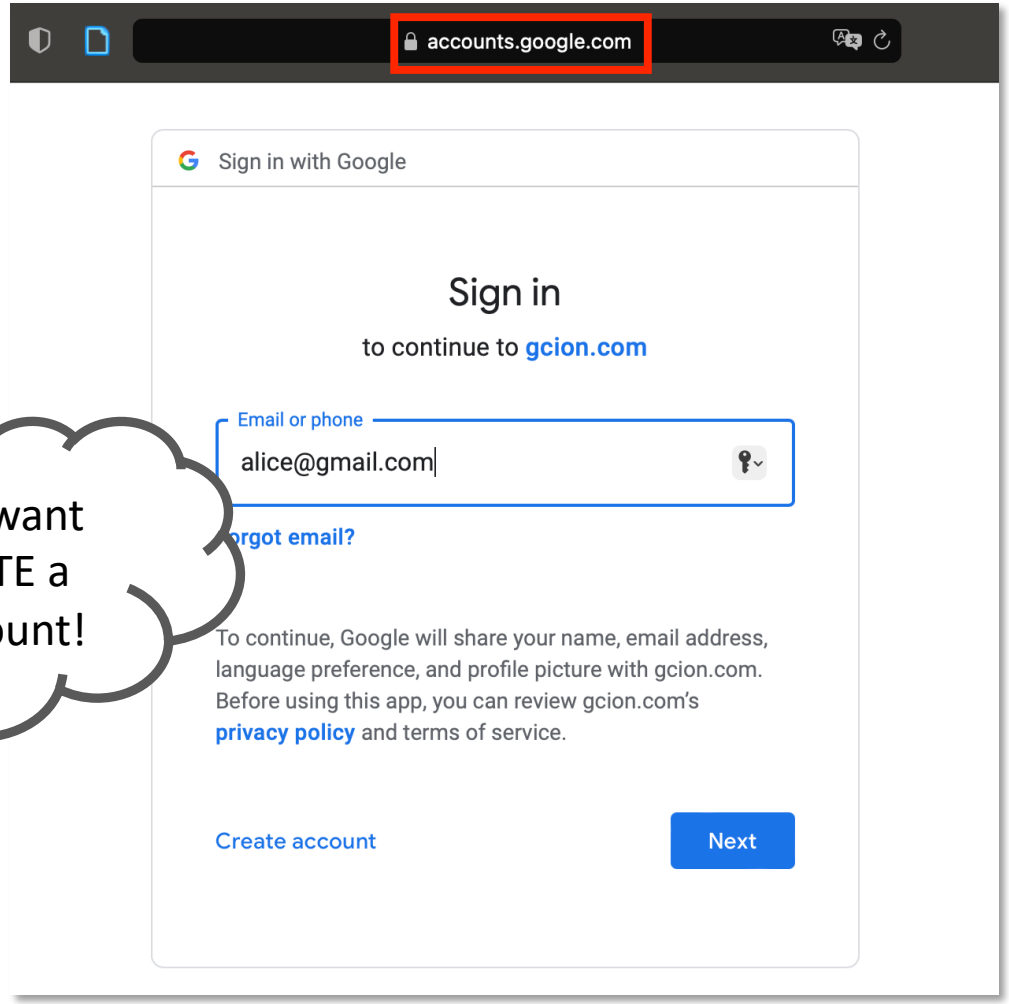
†Yale University




What is Single Sign-on (SSO)?







3rd Party App (RP) you want to log in…

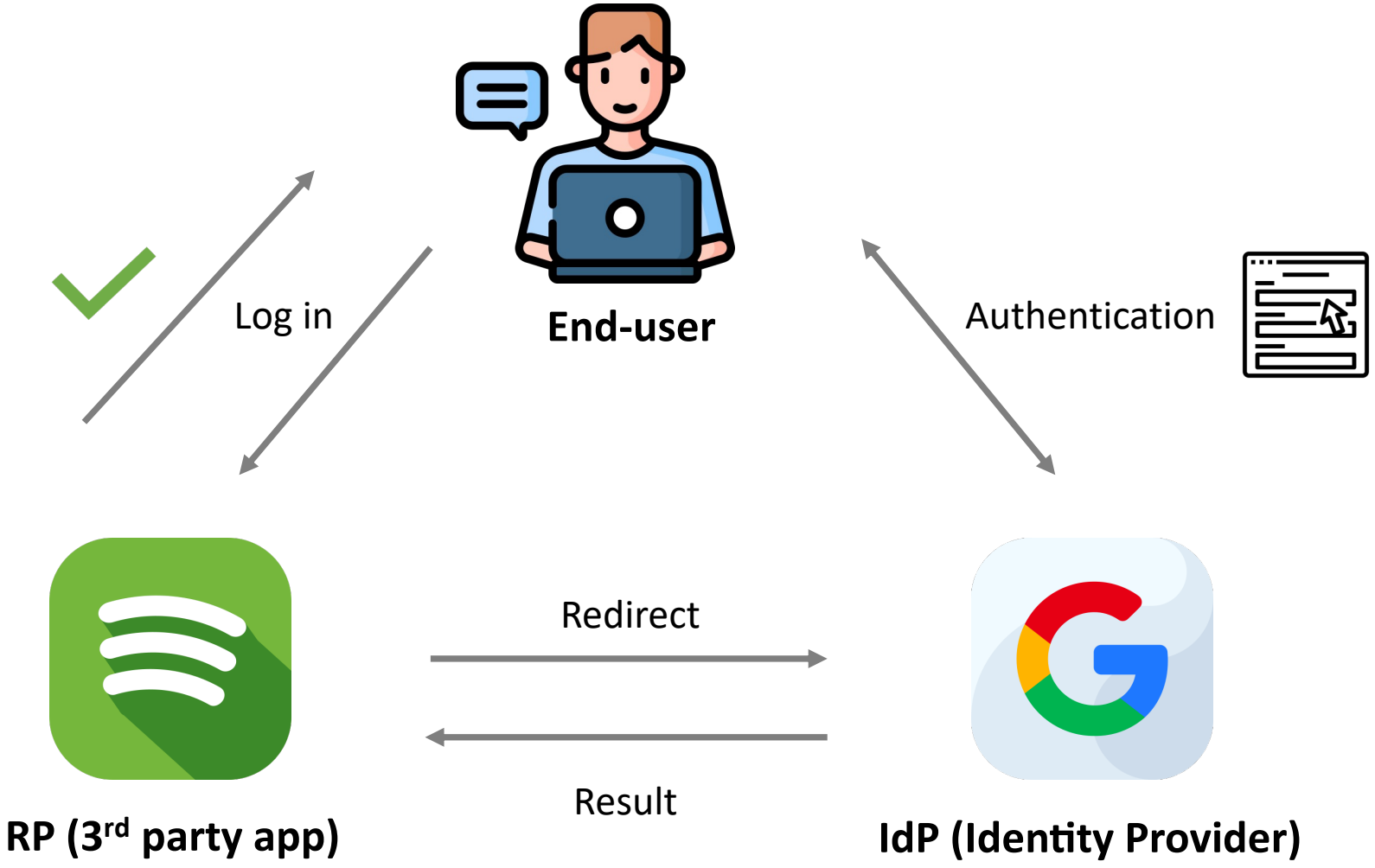
…just authenticate with the Identity Provider (IdP)

Pros & Cons of SSO

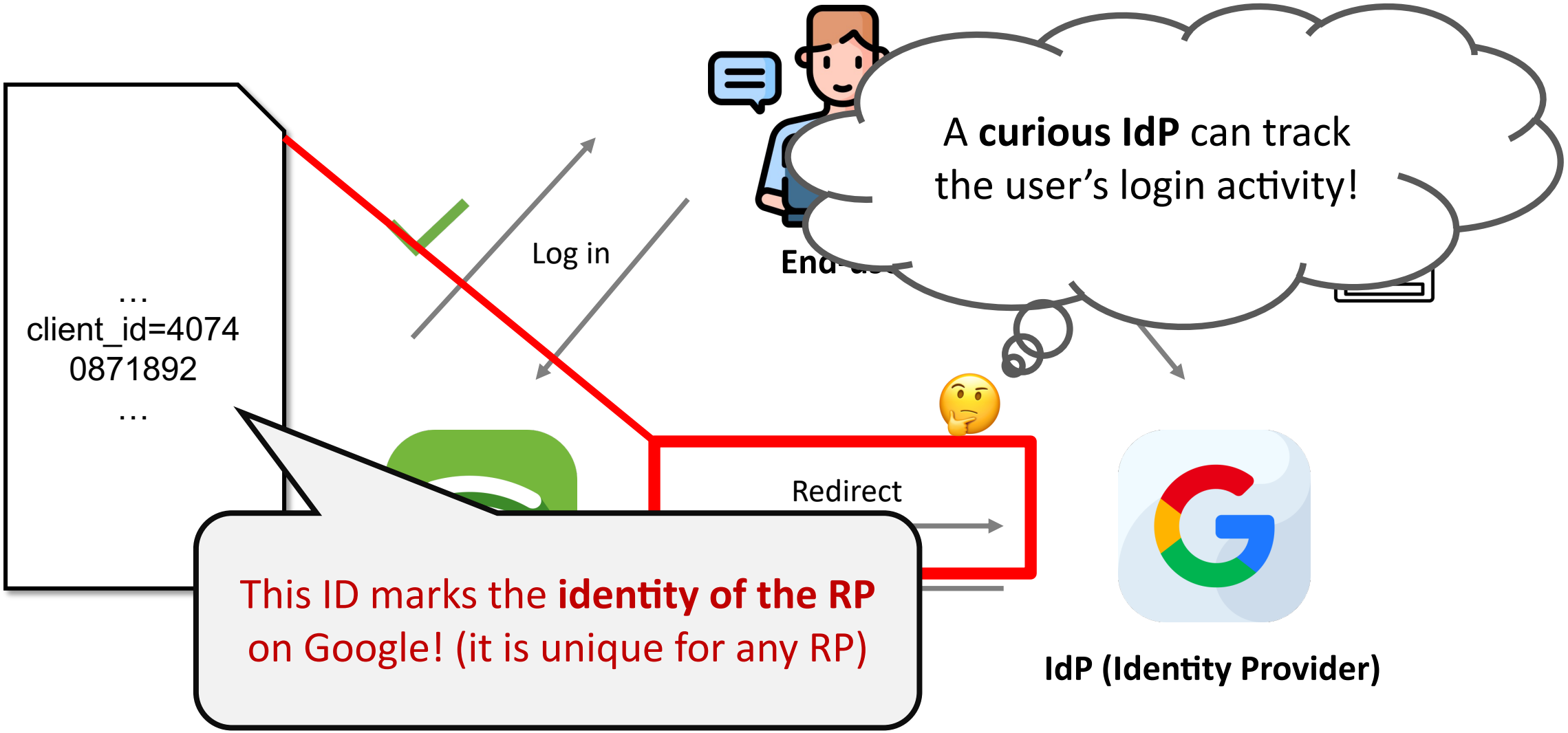
- ✅ Advantages
- Convenient: a familiar user experience without extra account registration
- Safety issues: fewer password reuses on such 3rd party apps
- Well-supported: 84,000+ apps support Google

- ❌ Drawbacks
- Many **Security & Privacy** issues!
  - Account linkage by IdP
  - Account linkage across RPs
  - Unnecessary identity exposure
  - Single-point failures of account security and availability

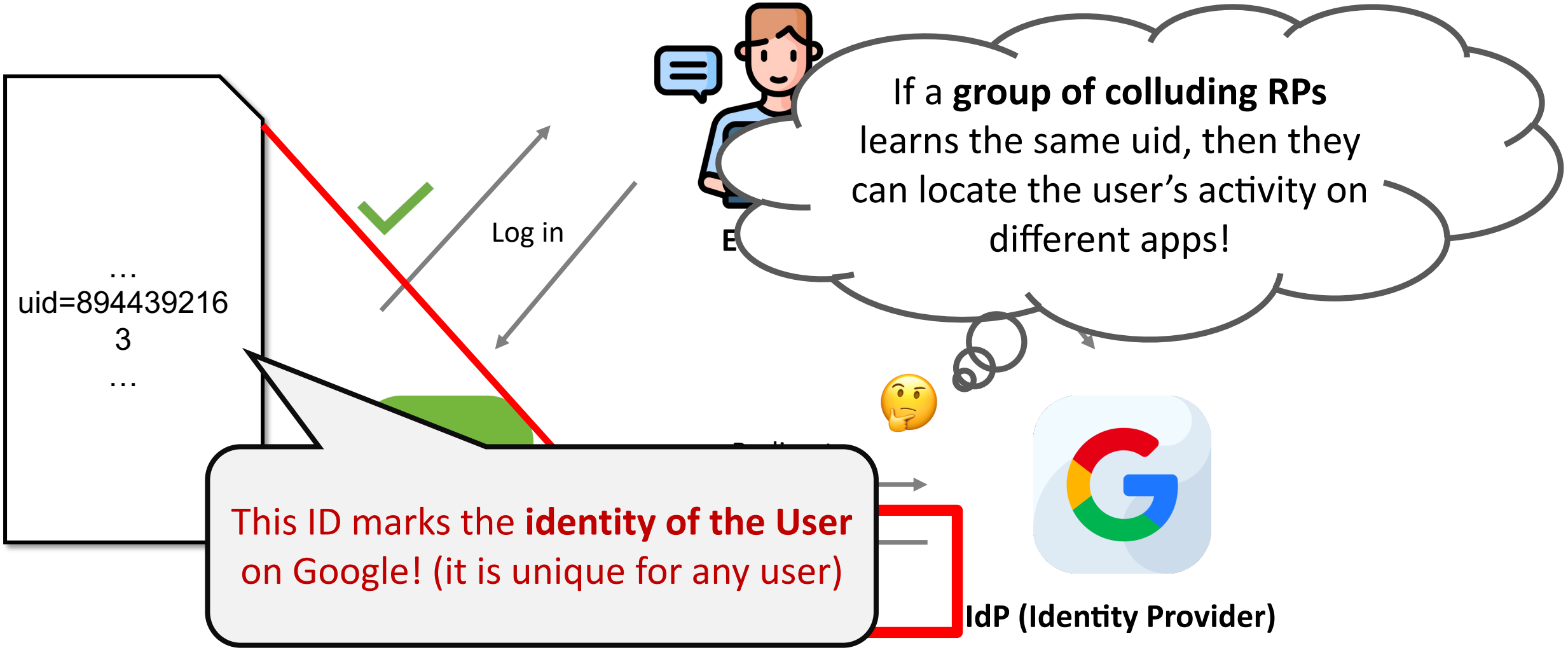
SSO in Details



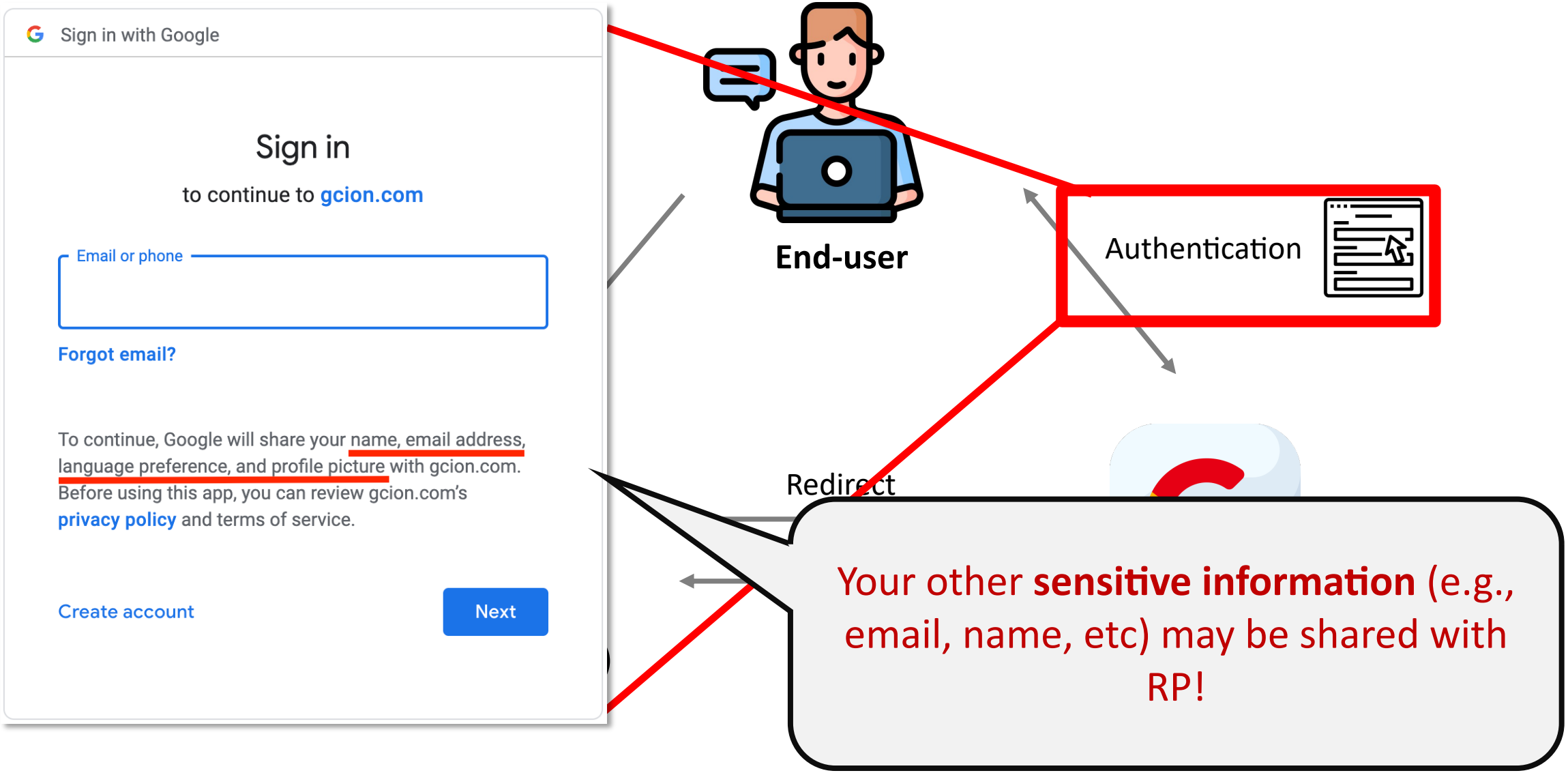
Issue I: Account Linkage (Tracking by IdP)



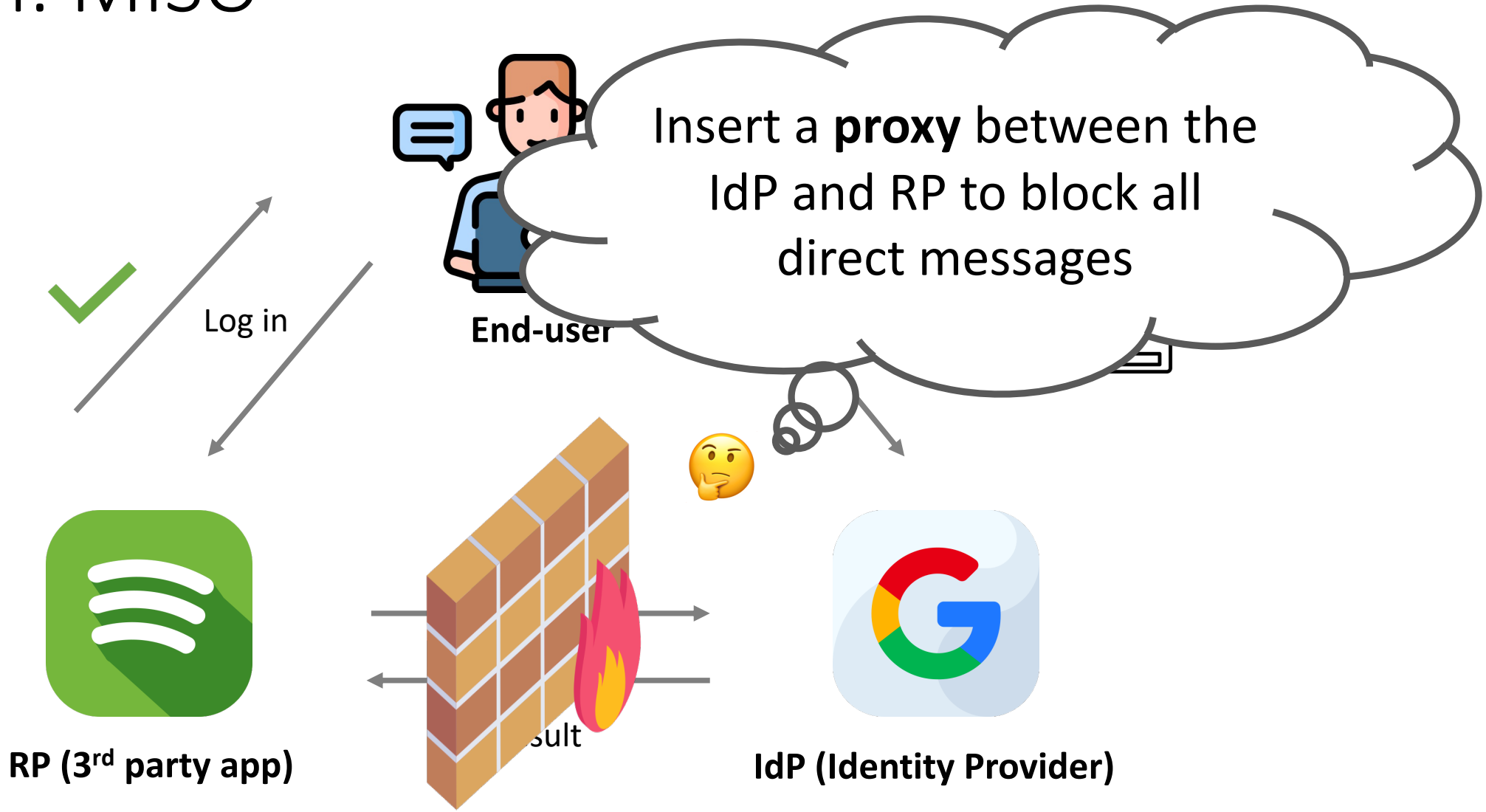
Issue II: Account Linkage (Tracking across RPs)



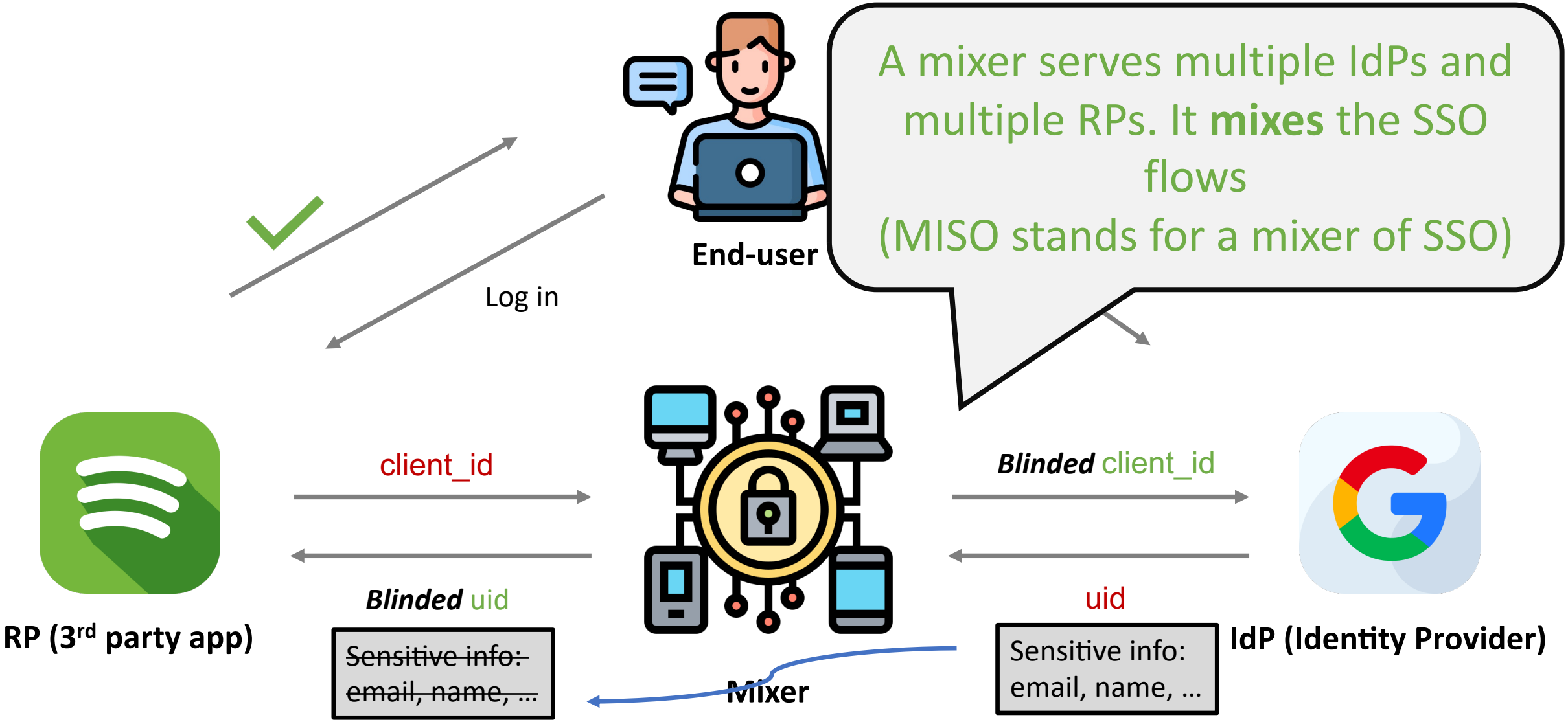
Issue III: Unnecessary Exposure to RP



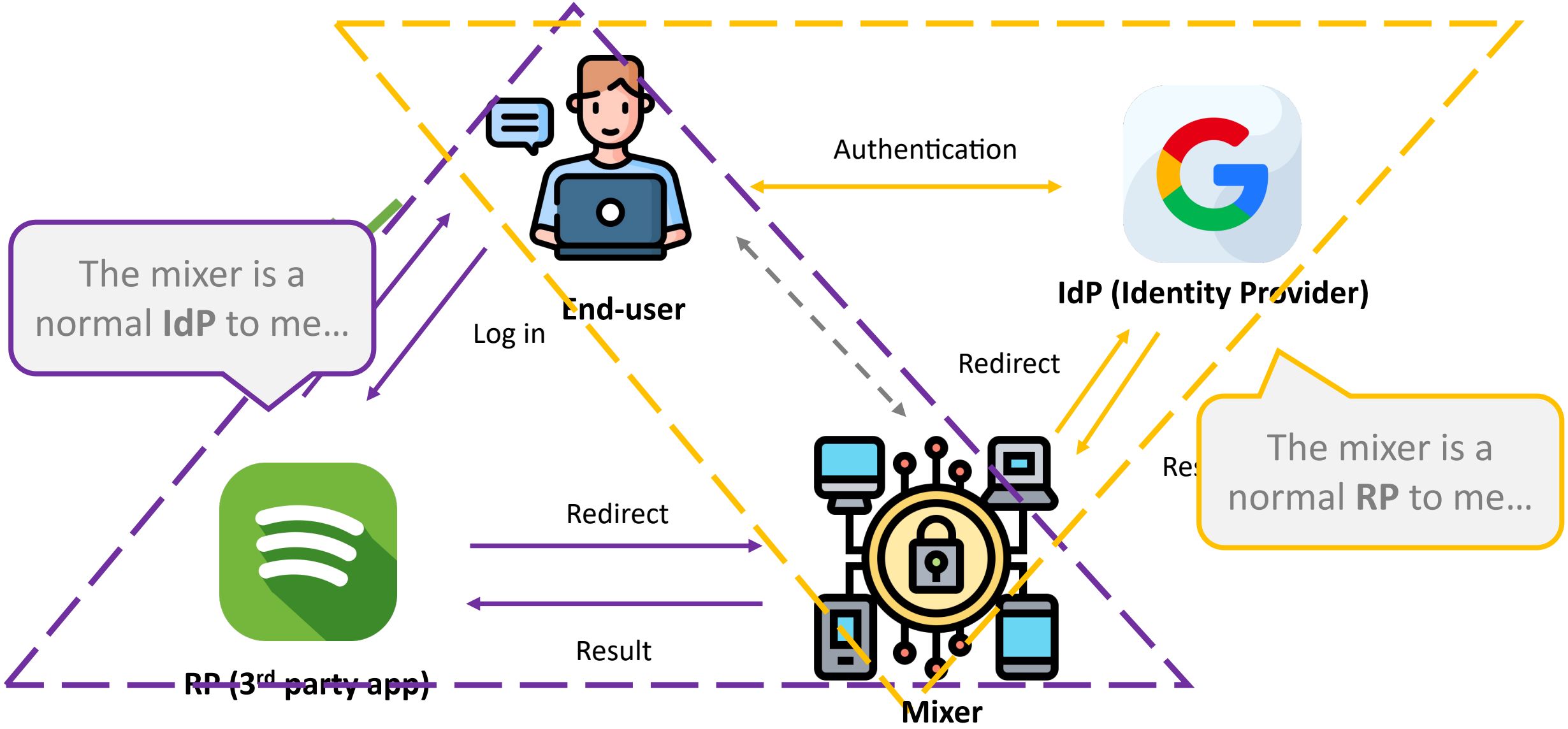
Solution: MISO



Solution: MISO



MISO: Two Nested SSO



Feature I: Privacy-preserving using Blinded Identifiers

- The Mixer is an RP to the Google and is an IdP to Spotify.
- The Mixer gets client_id_Mixer from Google (instead of Spotify), this ID **tells no information about Spotify**, which can be used as a blinded client_id.
- The Mixer gets uid from Google. Blind it use:
- $uid_{blinded} = PRF(sk, uid||client\_id\_RP||salt)$

Pseudo-random function

Fixed random key

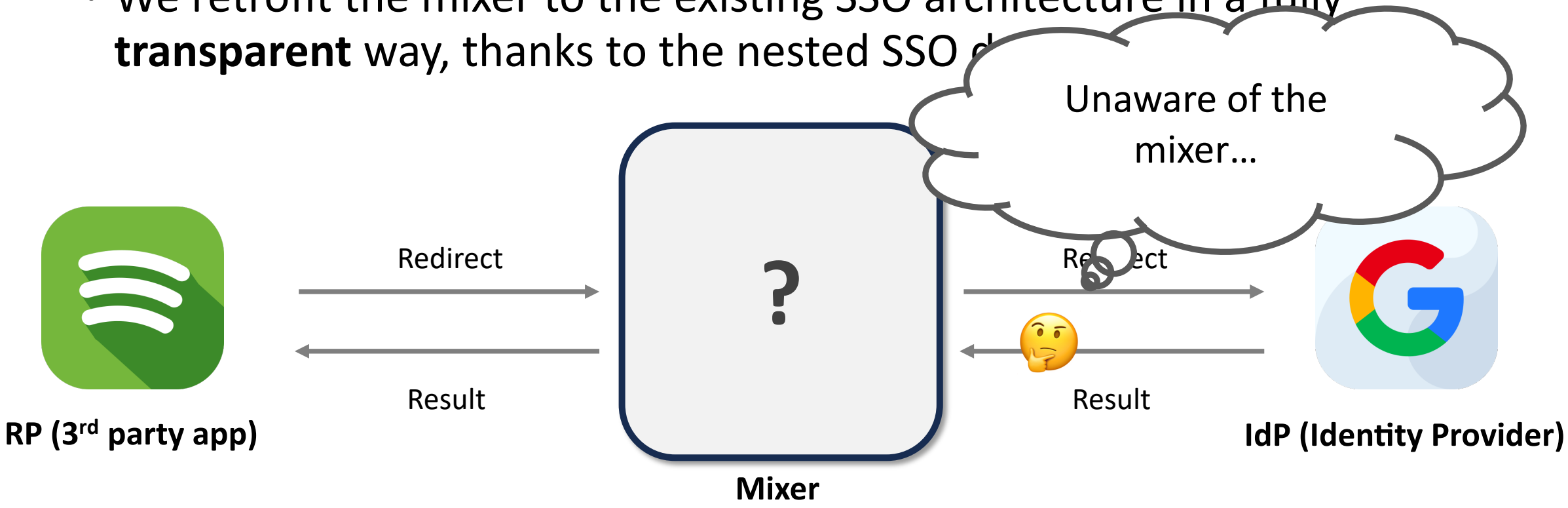
RP's client_id at the Mixer

Salt to prevent Rainbowtable attack

This blinded uid **tells no information about the User.**

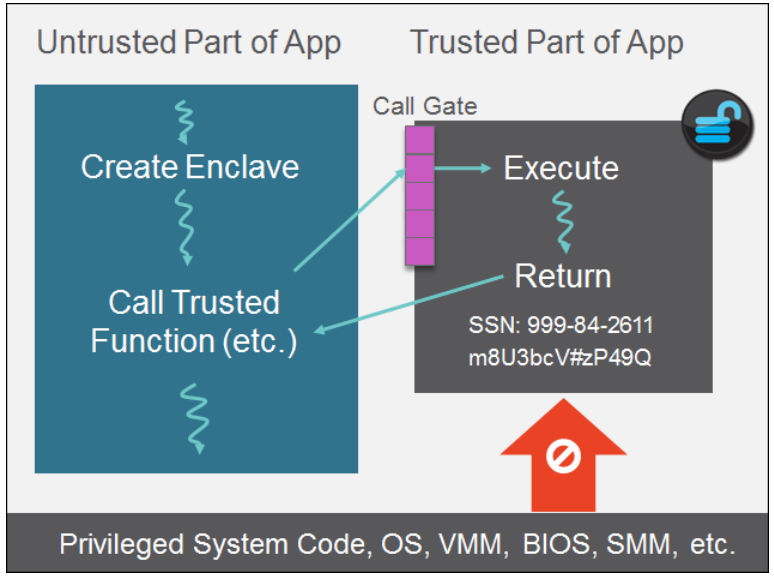
Feature II: MISO is Backward Compatible

- The system is **completely backward compatible** with deployed SSO systems.
- We retrofit the mixer to the existing SSO architecture in a fully **transparent** way, thanks to the nested SSO d



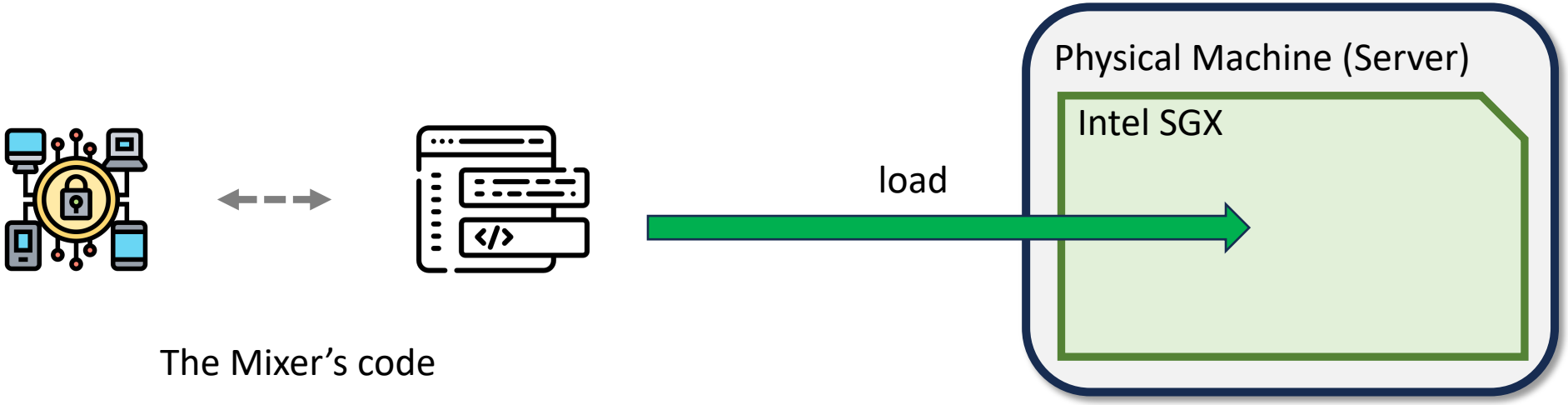
Feature III: MISO is Trustworthy

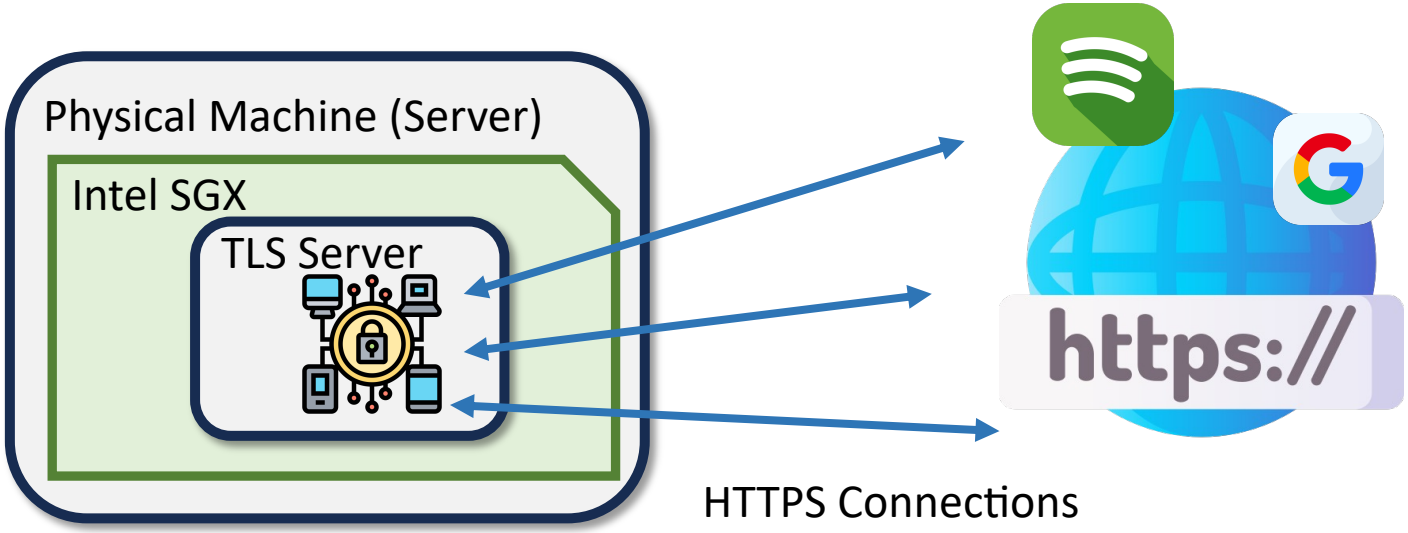
- **The Mixer is fully trusted**
- The Mixer can keep the confidentiality and integrity of its code and data
- The Mixer can complete its duty (described in code) without missing a beat.



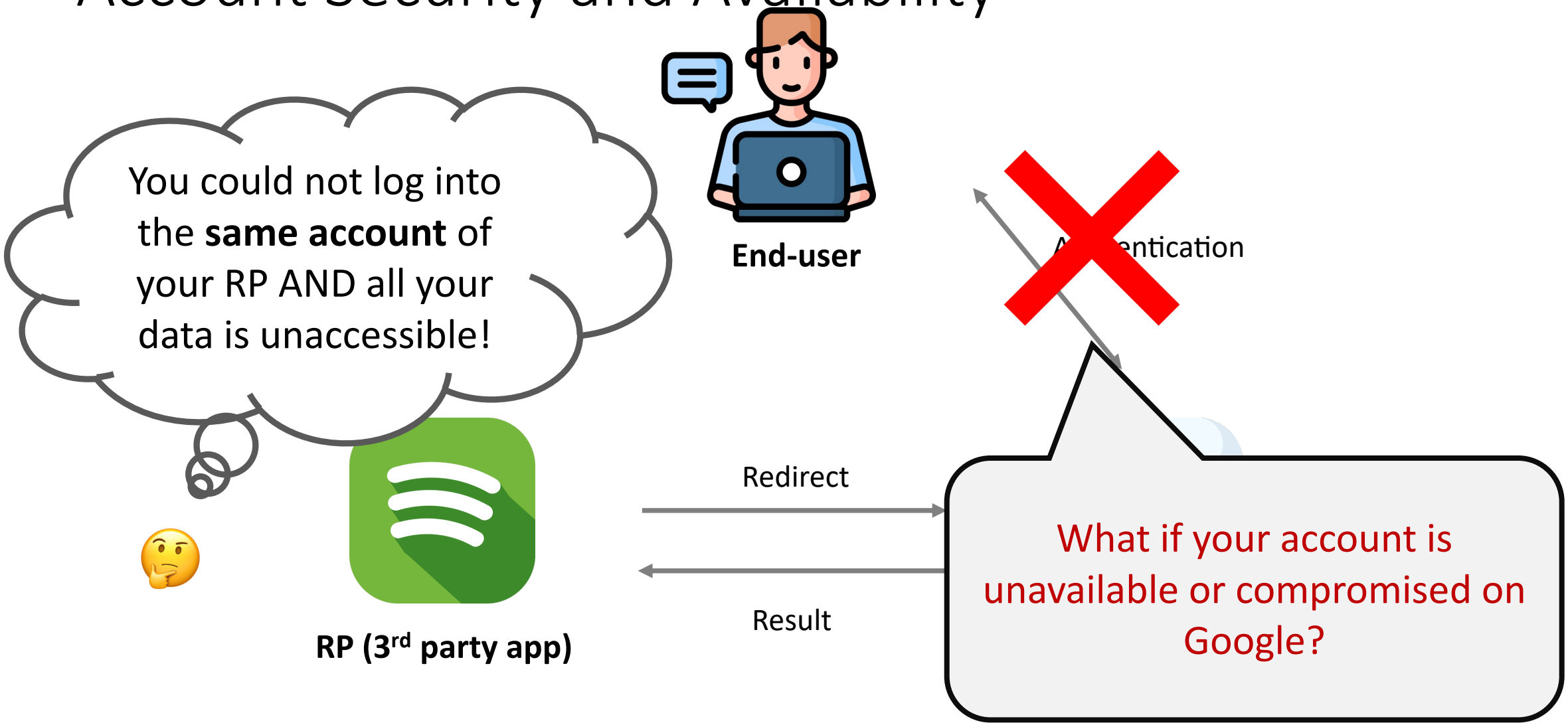
Trusted Execution Environment, e.g., Intel SGX, can be used to safeguard the Mixer

Feature III: Using TEE to Safeguard the Mixer





One More Problem: Single-point Failures of Account Security and Availability



Extension: (Multi-IdP) MISO

The mixer **saves and checks** the IdP authenticate information.

Users can choose to authenticate in a **threshold fashion**, e.g., 2 of 3 of the IdPs.

Less secure, since the Mixer needs to keep the information

RP (3rd party app)

Result

Mixer

Redirect

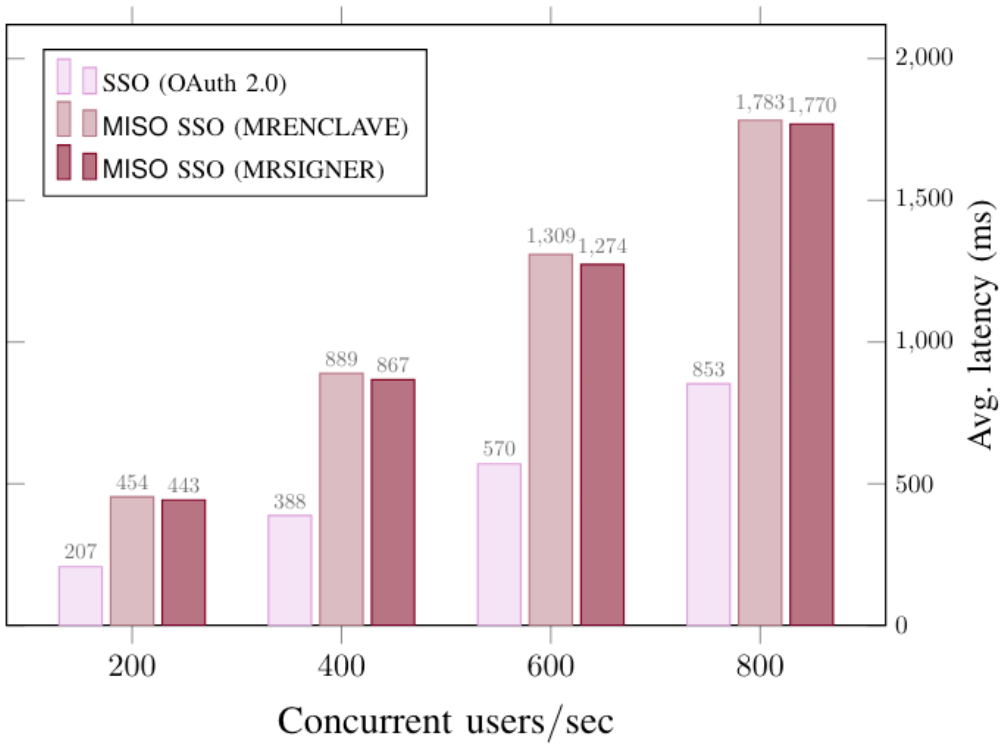
Result

IdPs

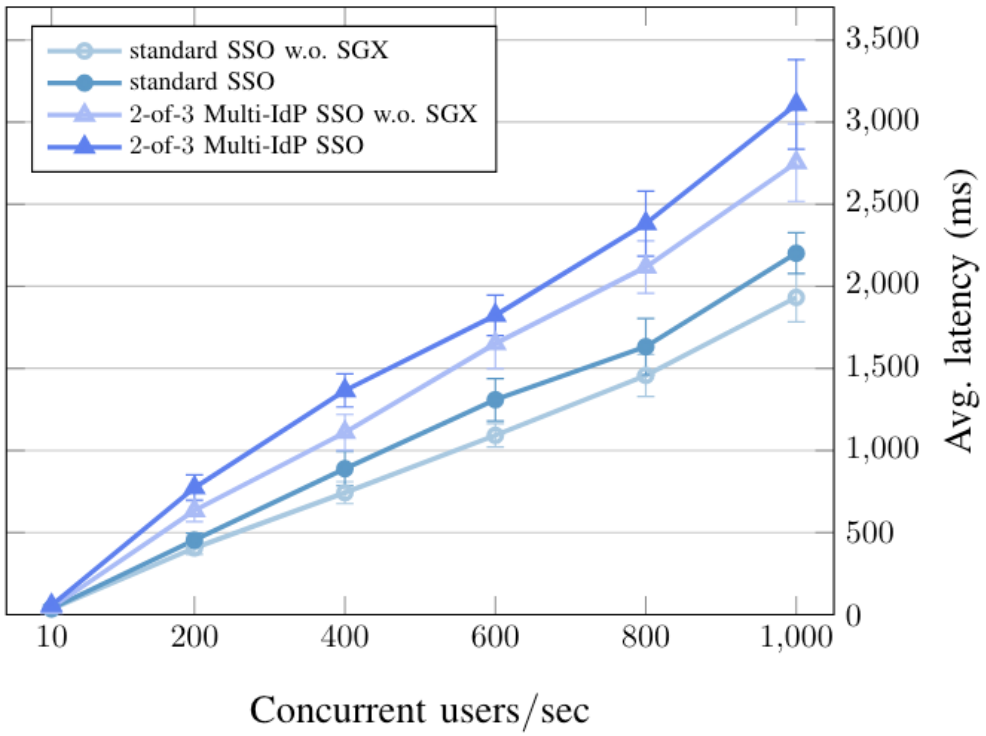
Implementation

- The Mixer is implemented in Golang, supported by EGo for SGX libOS.
- Server: 30GB ram, SGX enabled.
- All connections using TLS, X.509 certificates are installed on our server.
- Tested with Google, Facebook, and Github as IdPs.

End-to-end Performance



MISO roughly incurs 2× more latency when compared with the normal SSO



The involvement of SGX brings less than 15% extra overhead

Conclusion

- We propose the first **legacy-compatible privacy-preserving** SSO
- MISO achieves four security and privacy goals:
  - user account unlinkability by the IdP
  - unlinkability across RPs
  - selective disclosure of user identity
  - robust to single-point of failures (w.r.t. account availability)
- Our prototype implementation and evaluation suggest that MISO enjoys high usability in real-world applications

Thanks for listening!

Contact Rongwu Xu for more details

xrw22@mails.tsinghua.edu.cn

arXiv full version