OAuth Redirect Security

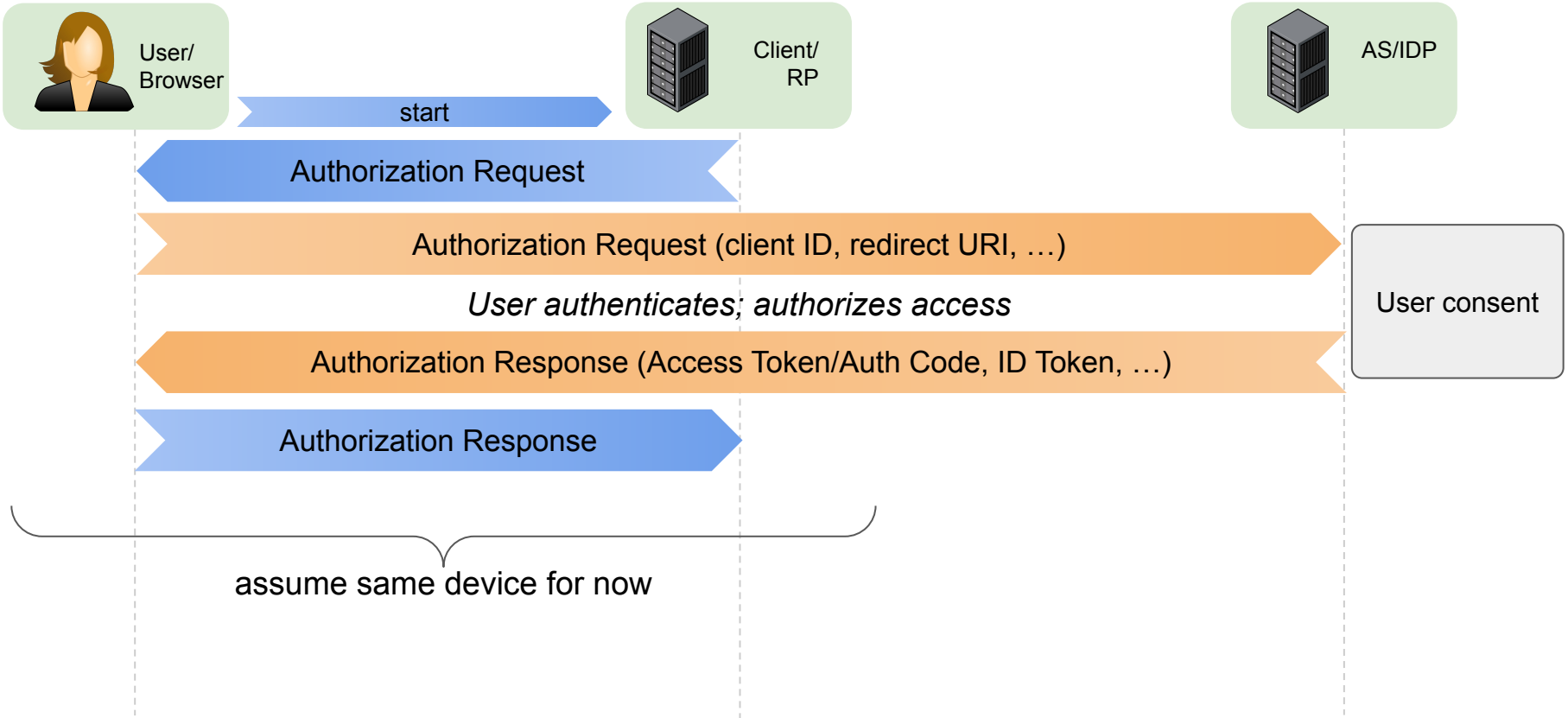
Dr. Daniel Fett

yes®

Dr. Daniel Fett

- Security specialist at yes.com
- Working groups:
  - IETF: OAuth
  - OpenID Foundation: OpenID Connect
  - OpenID Foundation: Financial-grade API Security Profile
  - OpenID Foundation: eKYC and Identity Assurance
- Formal analysis of web security

Redirect-based Flows



(Selected) Attacks

Auth Request MITM
Attacker forwards an auth request to a user who then completes the flow on the attacker’s behalf.

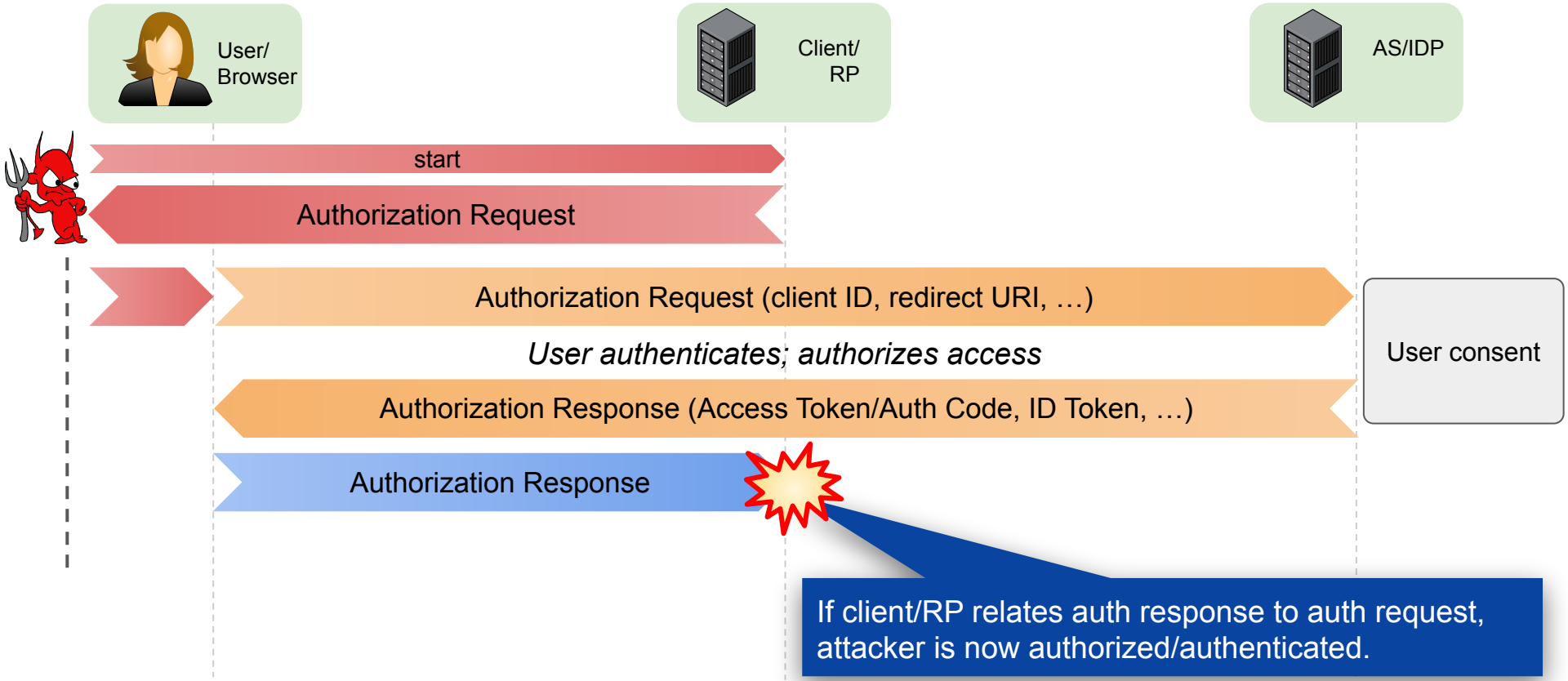
CSRF
Attacker uses a credential issued for themselves and tries to inject it into a flow on a user's device between the user and a verifier.

Exfiltration of Personal Data (ID Token, VP Token)
The exfiltration of personal data without the user's (proper) consent.

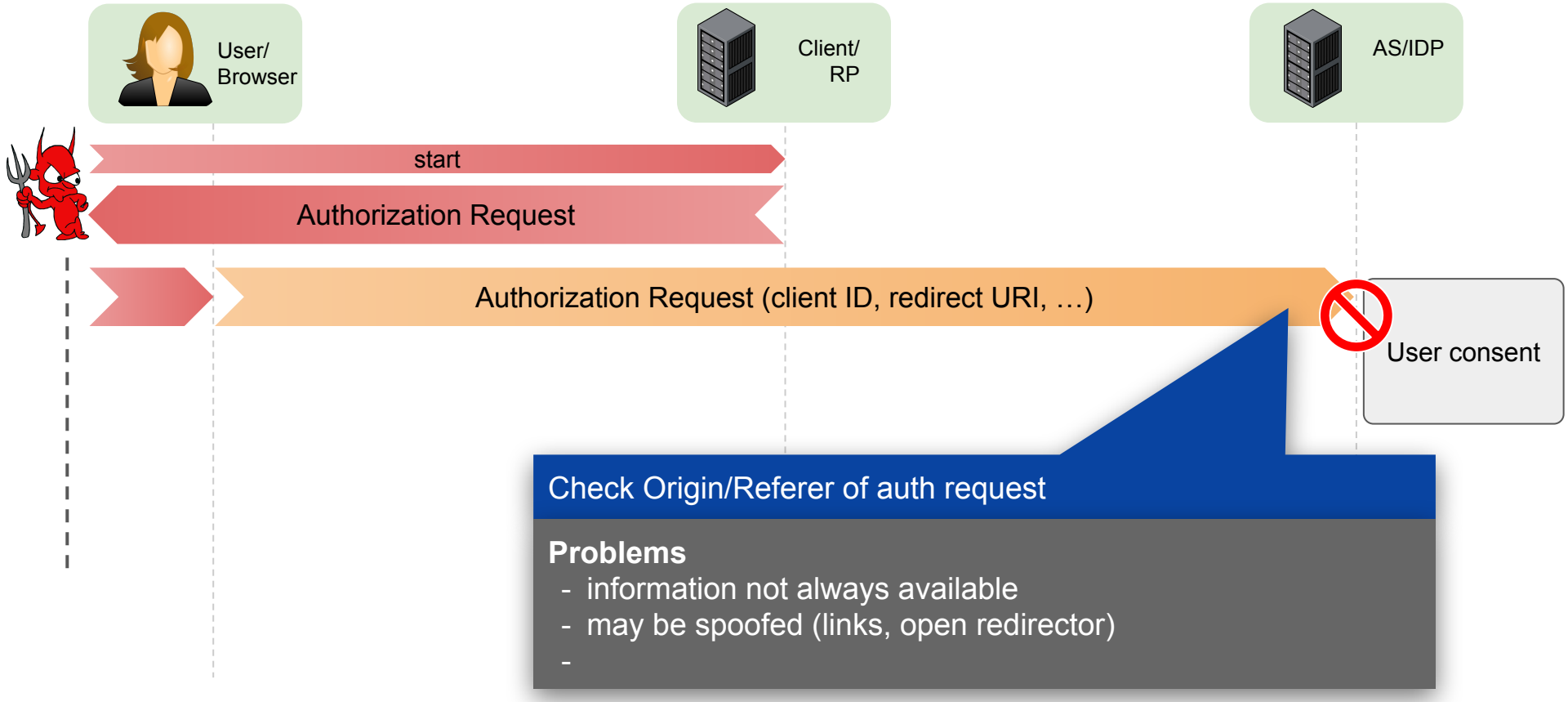
Injection
Attacker uses an exfiltrated credential issued for a user and tries to inject it into a flow on the attacker's own device to mislead a verifier.

Auth Request MITM

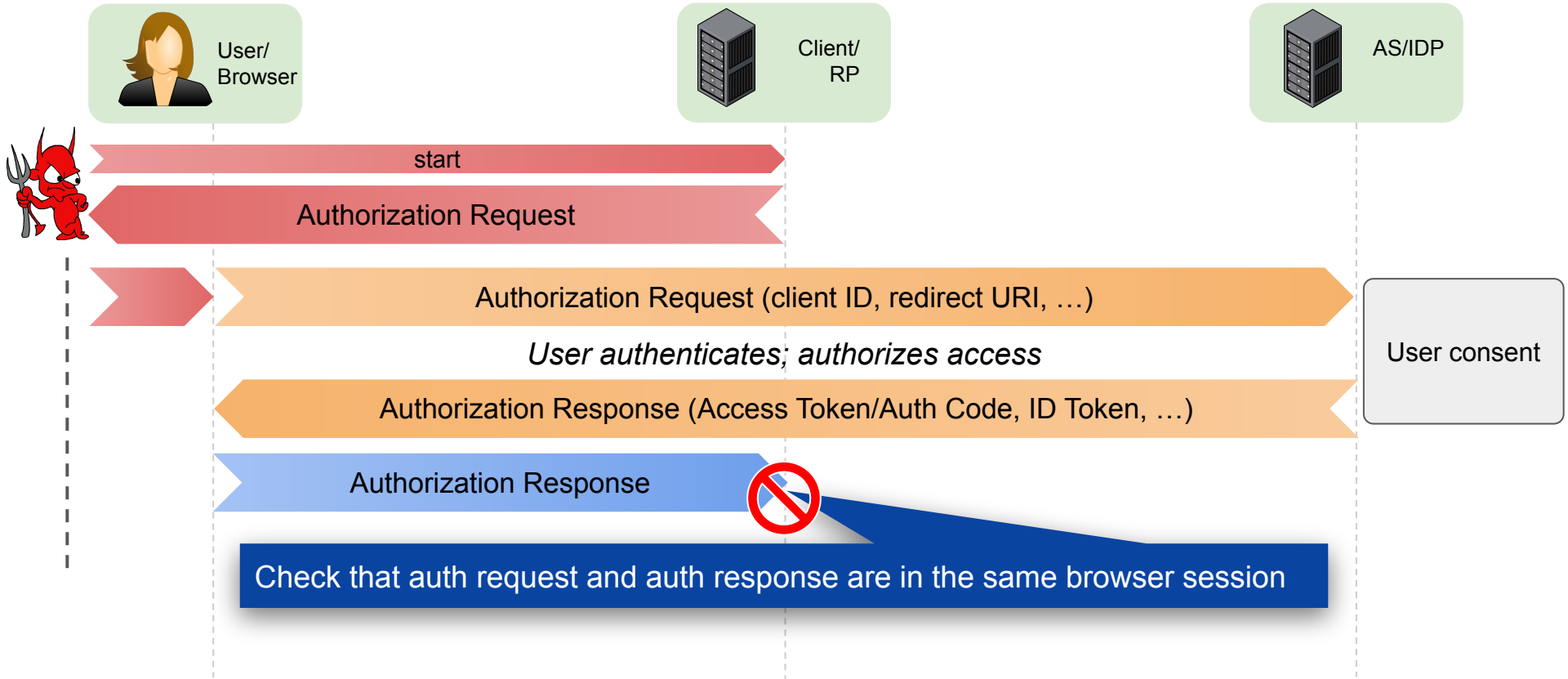
Auth Request MITM



Auth Request MITM - Countermeasures - Option 1



Auth Request MITM - Countermeasures - Option 2



What about Cross-Device Flows?

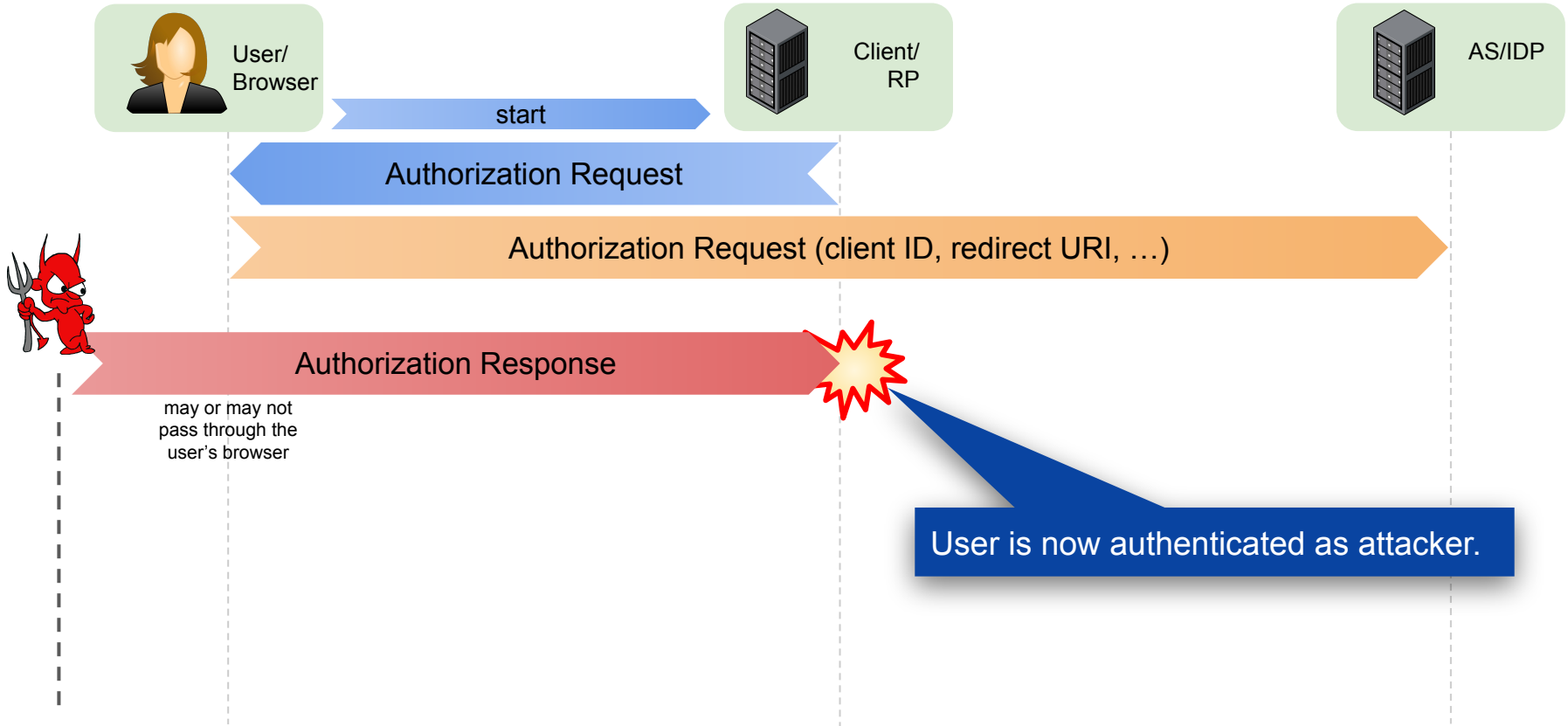
In cross-device flows, both Option 1 and Option 2 break.

Independent of concrete protocol.

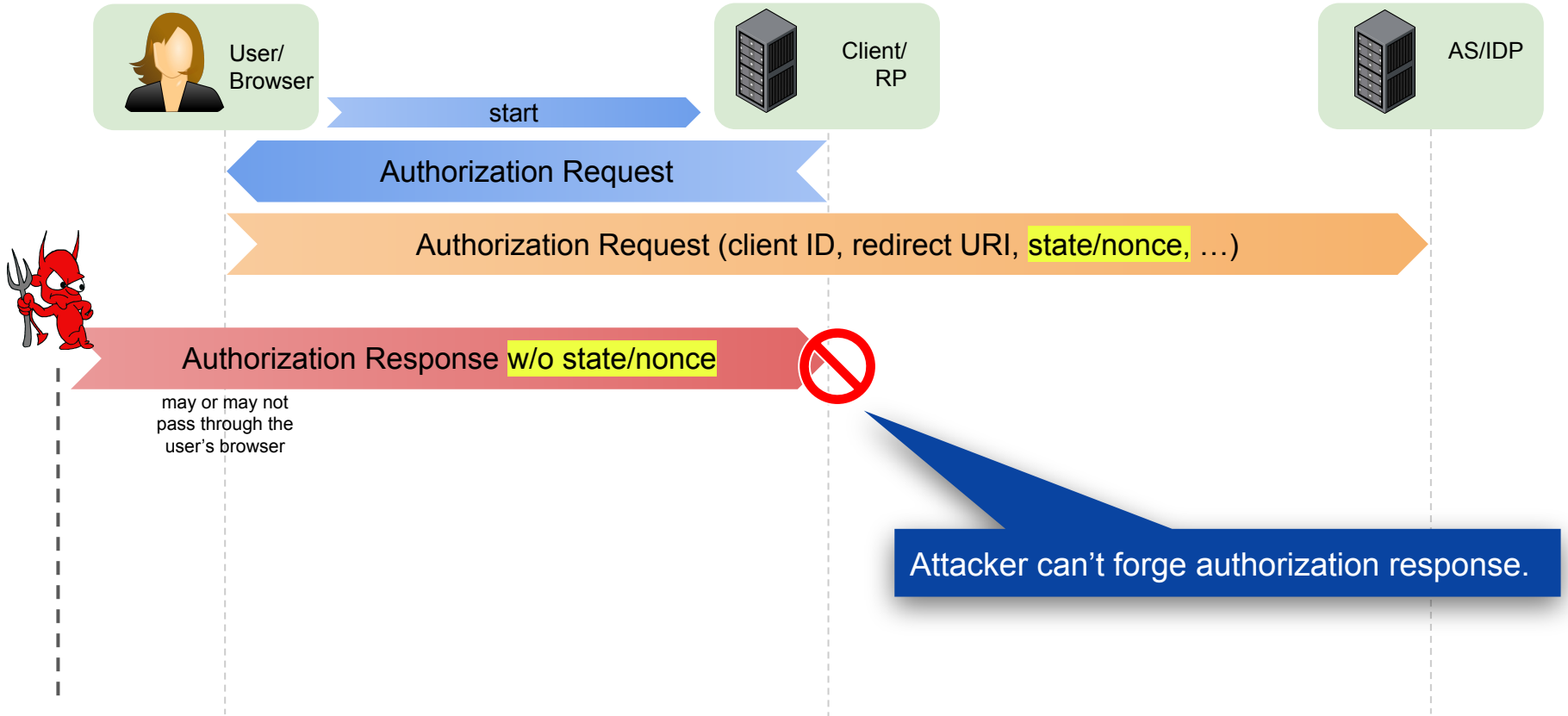
We are working on solutions…

CSRF

CSRF

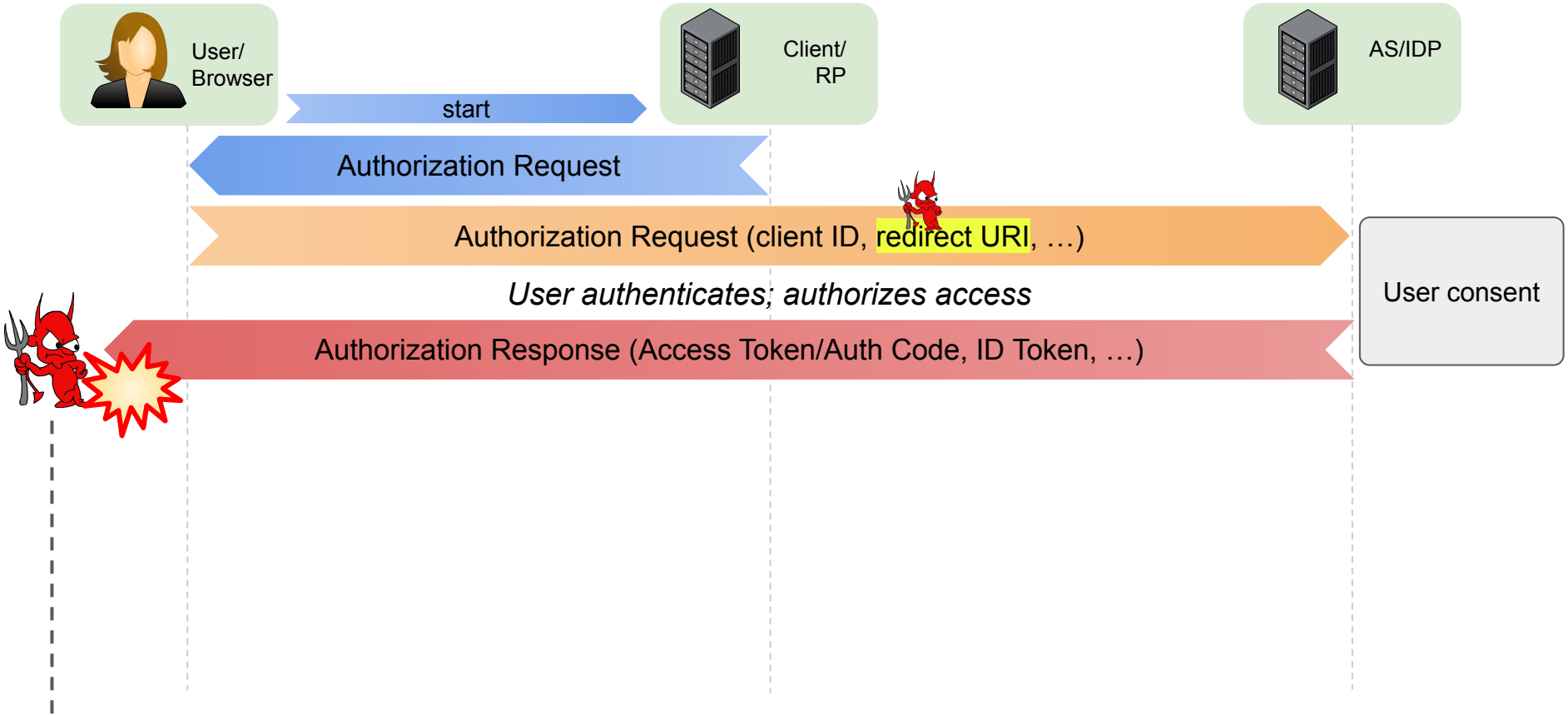

User/
Browser
Client/
RP
AS/IDP
start
Authorization Request
Authorization Request (client ID, redirect URI, …)
Authorization Response
may or may not
pass through the
user's browser
User is now authenticated as attacker.

CSRF - Countermeasures

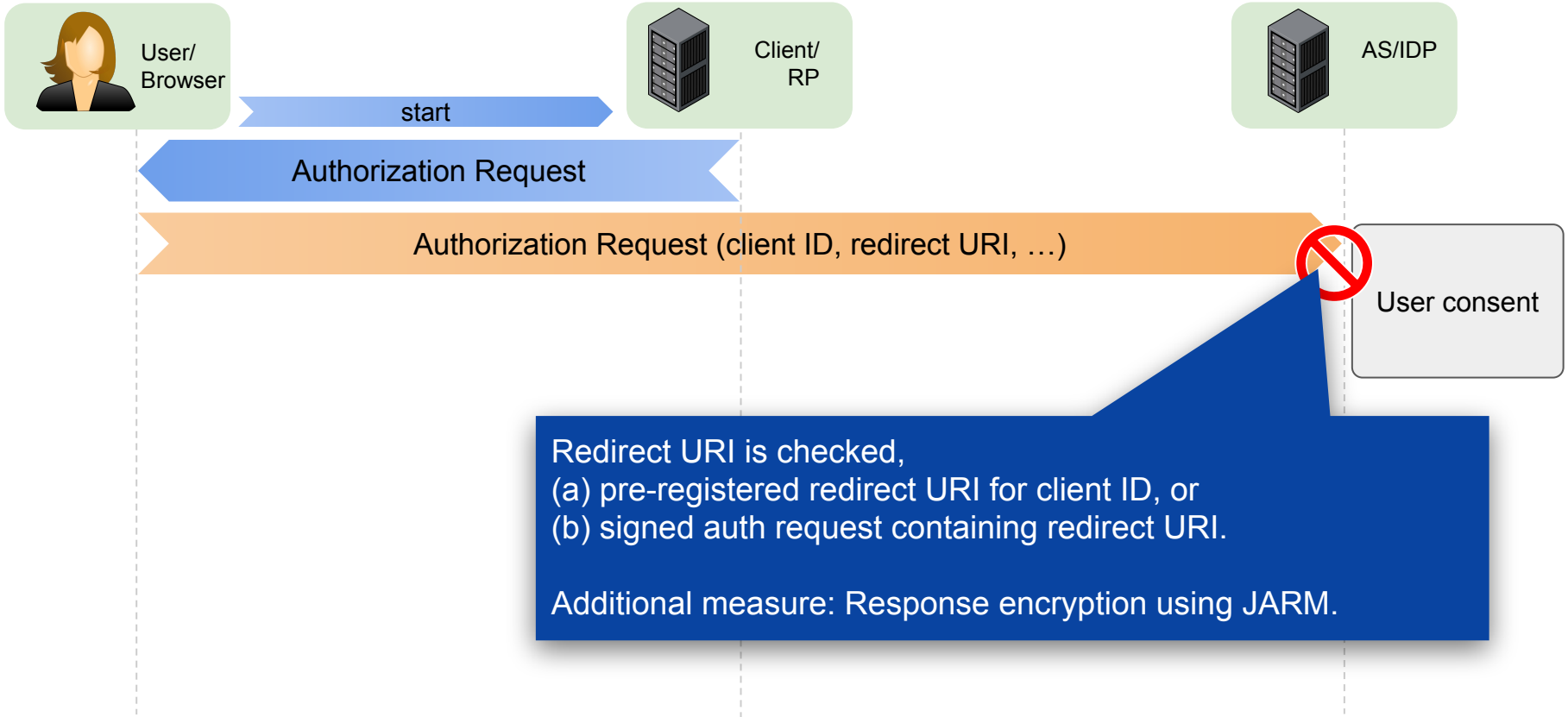


Exfiltration of PII

Exfiltration of PII

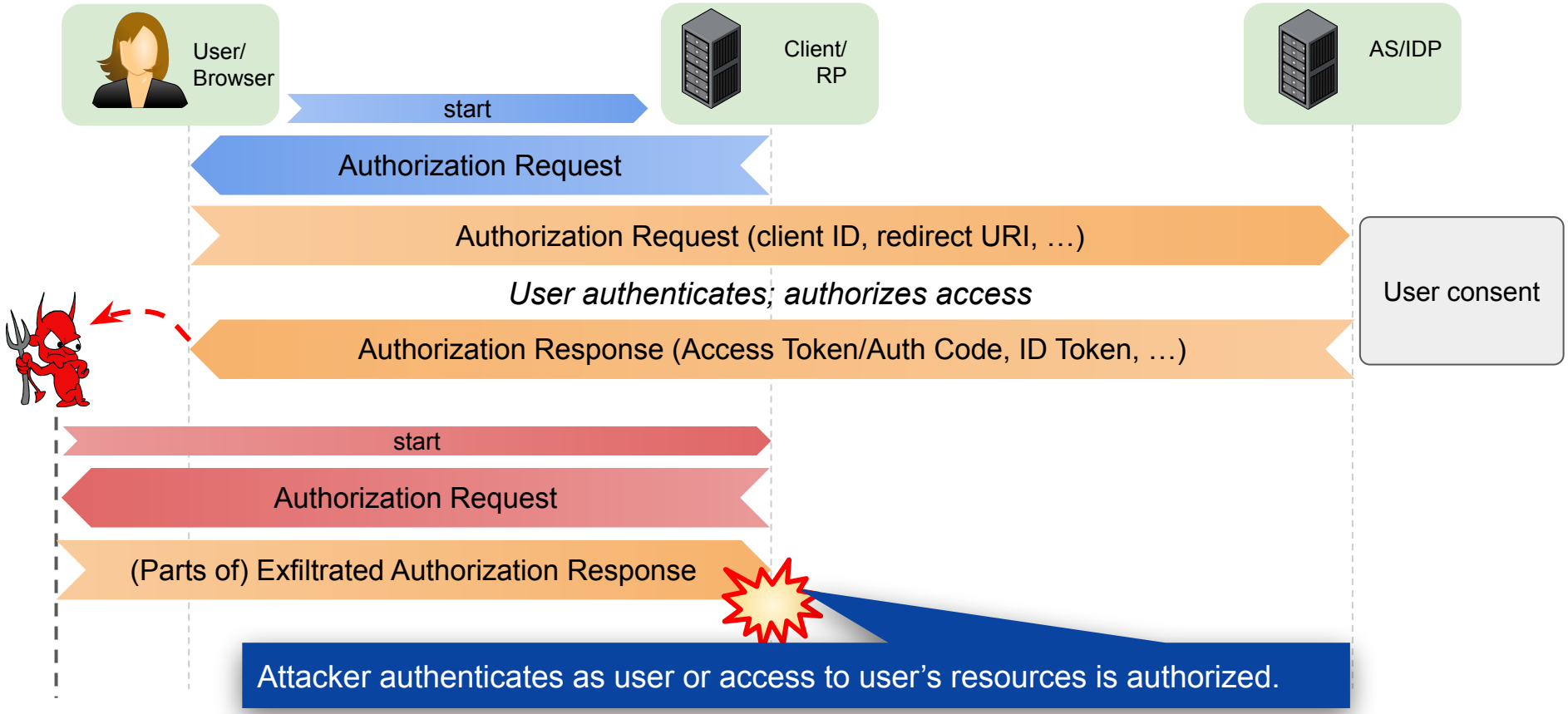


Exfiltration of PII - Countermeasures



Injection

Injection Attack



Injection Attack - Countermeasures

- For access token: Don’t use frontchannel flow
- For ID Token & VP Token:
  - Ensure that token must be obtained for the correct client (Audience Restriction/”aud”)
  - Ensure that token is bound to transaction (Nonce)

Dr. Daniel Fett
yes.com
danielf@yes.com
@dfett42

yes®