Privacy-Preserving Single Sign-On

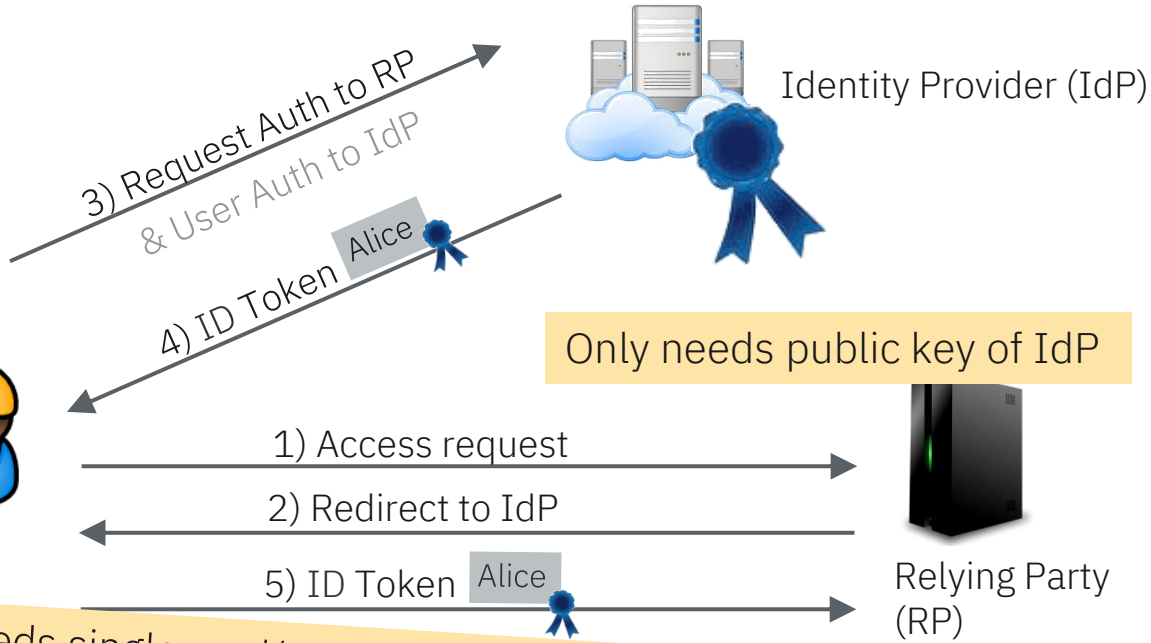
Attributes & Blindness Workshop @ Eurocrypt 2024
26.5.2024

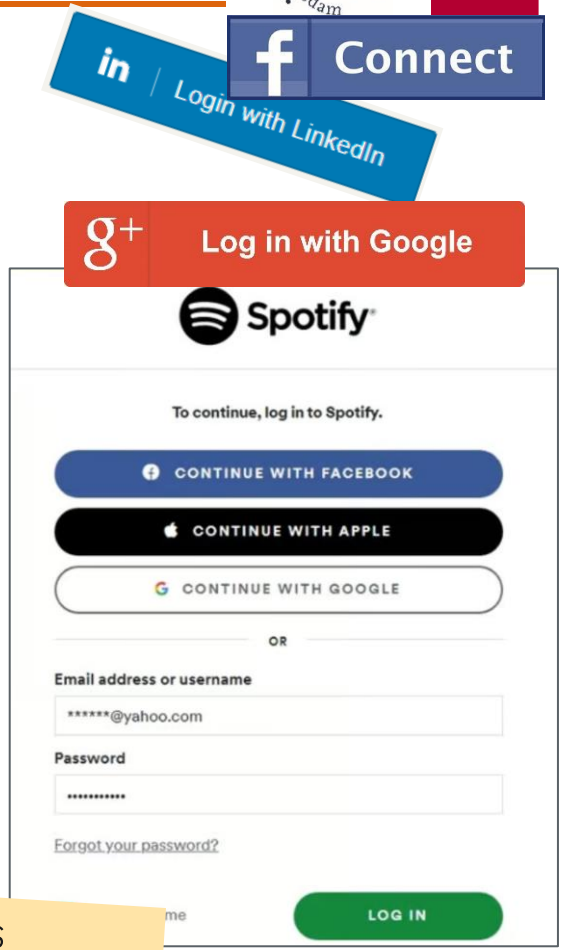
Anja Lehmann

Hasso Plattner Institute | University of Potsdam

Single Sign-On | Convenient User Authentication

- Authentication outsourced to Online Identity Provider
  User → IdP: password/2FA. Single pwd, no credentials/keys!
  User → RP: relayed ID token signed by IdP

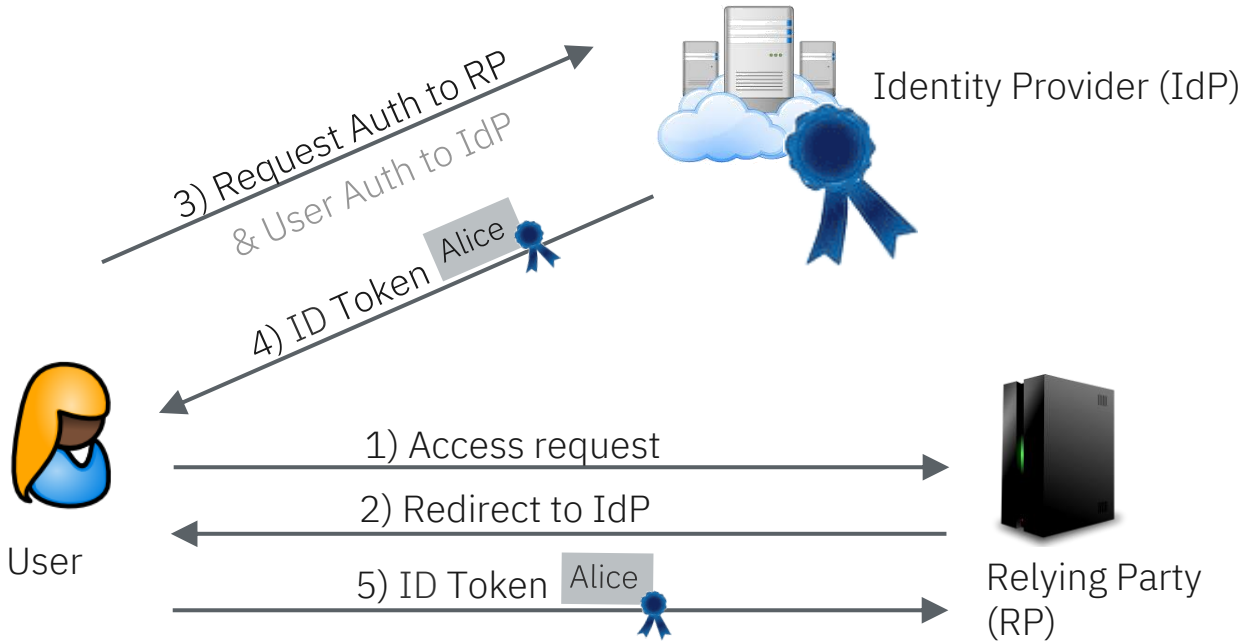




Only needs single pwd/2FA towards IdP → authentication to many RPs

Single Sign-On | Strong User Authentication

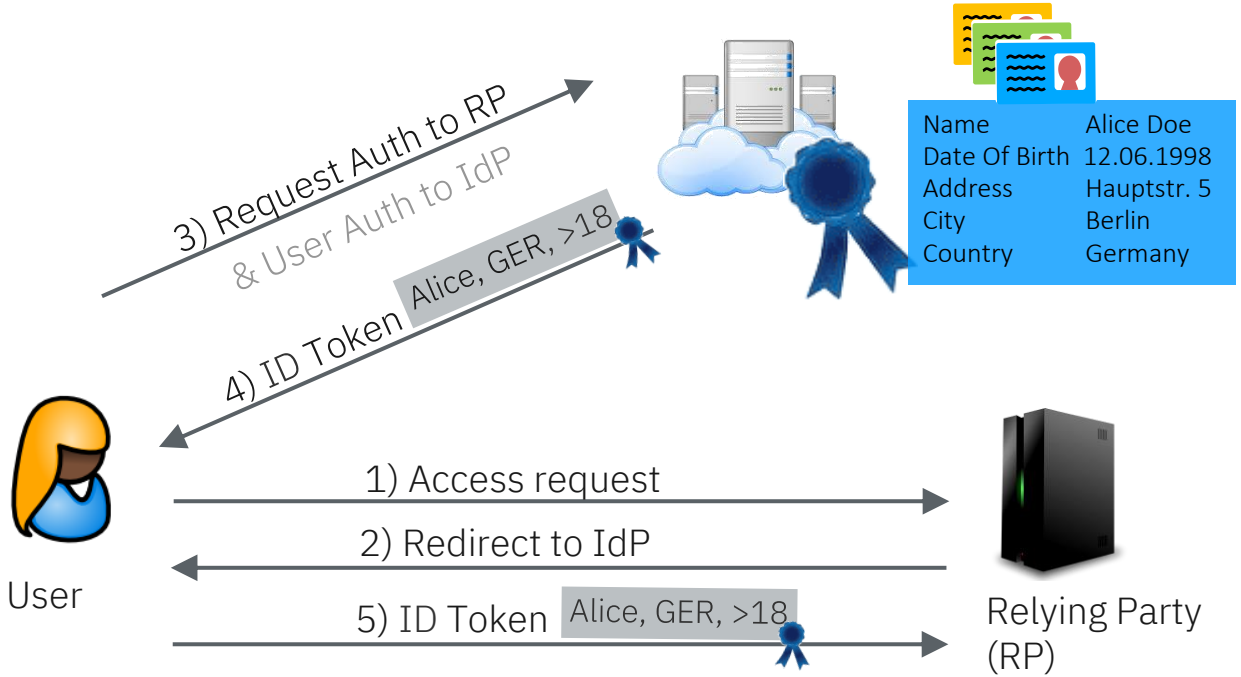
- ID Token signed by IdP → security through unforgeable signatures
  - attests necessary user information
  - bound to session & RP



Properties	SSO
Usability	✓
Strong Authentication	✓

Single Sign-On | Selective Disclosure & Strong Auth

- IdP knows several verified user attributes
  & attests only minimally necessary user information



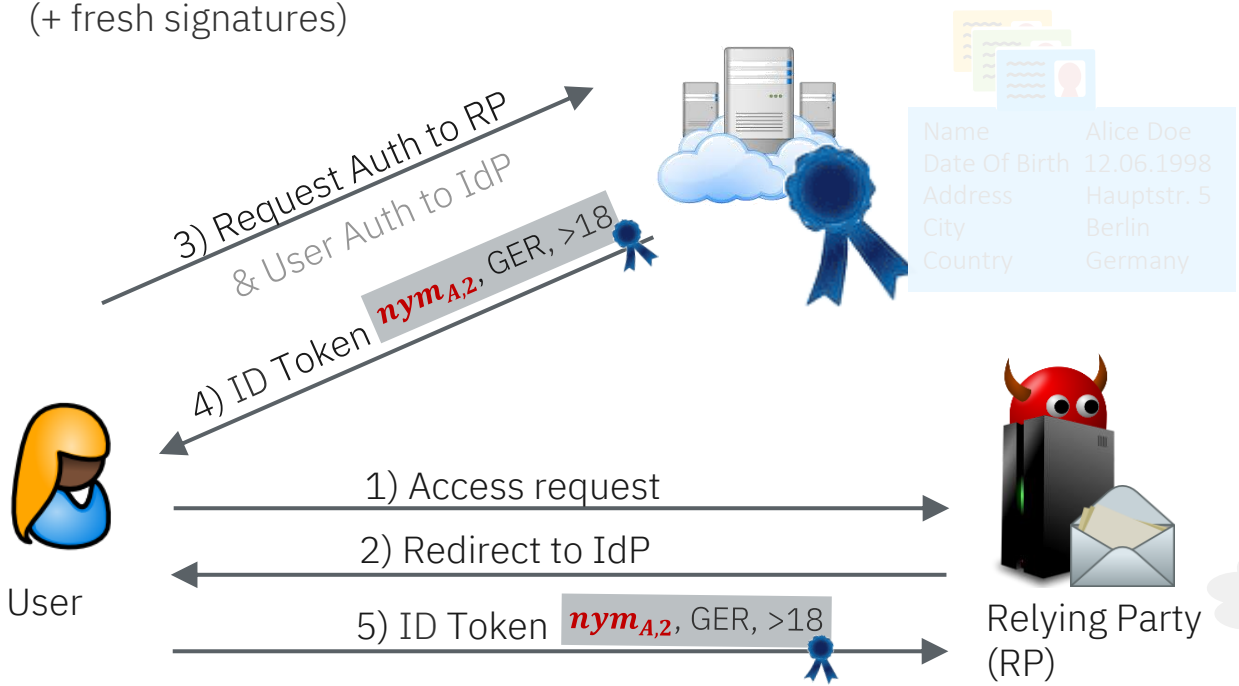
Properties	SSO
Usability	✓
Strong Authentication	✓
Selective Disclosure	✓

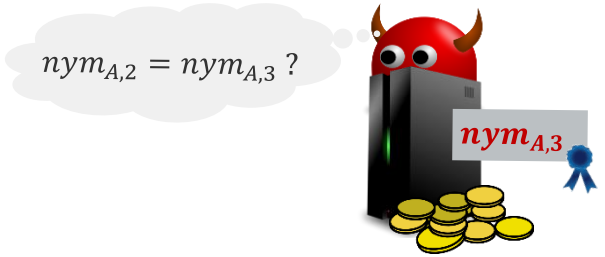
Single Sign-On | Unlinkability through Pseudonyms (PPID)

- Unlinkability through “Pairwise Pseudonymous Identifier” (ppid in OIDC)
  Dedicated pseudonyms per RP → unlinkable across RPs
  (+ fresh signatures)

	Movies	Mail	Bank
Alice	$nym_{A,1}$	$nym_{A,2}$	$nym_{A,3}$
Bob	$nym_{B,1}$	$nym_{B,2}$	$nym_{B,3}$
Carol	$nym_{C,1}$	$nym_{C,2}$	$nym_{C,3}$

Properties	SSO
Usability	✓
Strong Authentication	✓
Selective Disclosure	✓
Unlinkability (RP)	✓

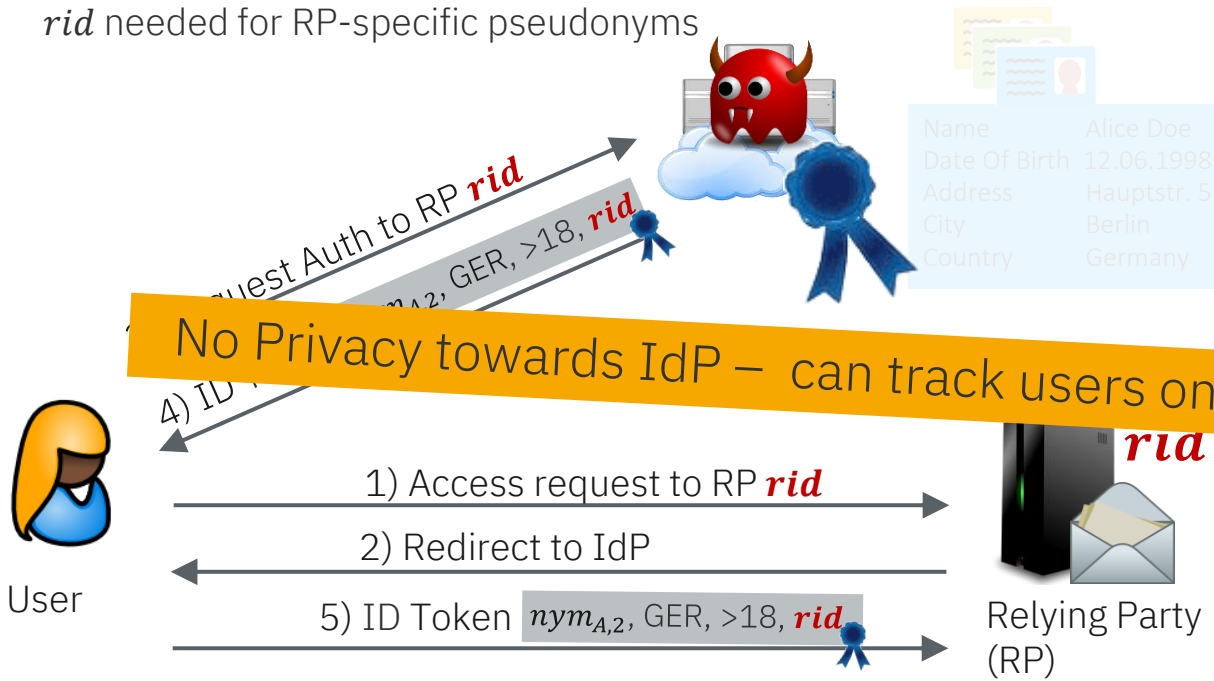




Single Sign-On | No Unobservability → RP Binding

- IdP needs to know the RP the user wants to authenticate to:
  binds token to specific RP rid → phishing prevention
  rid needed for RP-specific pseudonyms

	rid_1	rid_2	rid_3
Alice	$nym_{A,1}$	$nym_{A,2}$	$nym_{A,3}$
Bob	$nym_{B,1}$	$nym_{B,2}$	$nym_{B,3}$
Carol	$nym_{C,1}$	$nym_{C,2}$	$nym_{C,3}$



Properties	SSO
Usability	✓
Strong Authentication	✓
	✓
	✓
Unobservability (IdP)	✗

Single Sign-On | Achieving Unobservability

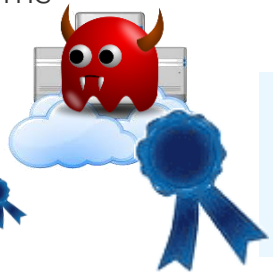
[HSB'20] Hammann, Sasse, Basin
Privacy-Preserving OpenID Connect
AsiaCCS'20

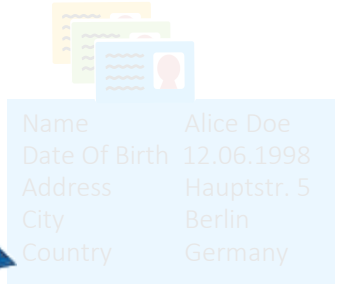

Sven Hammann
ETH Zurich


Ralf Sasse
ETH Zurich


David Basin
ETH Zurich

- ~~IdP needs to know the RP the user wants to authenticate to:~~
  Blindly binds token to specific RP rid
  Blindly derives RP-specific pseudonyms





3) Request for $c = H(rid, r)$

4) ID Token $nym_{A,2}$, GER, >18, c

User

1) Access request to RP rid

2) Redirect to IdP

5) ID Token $nym_{A,2}$, GER, >18, c, r

rid

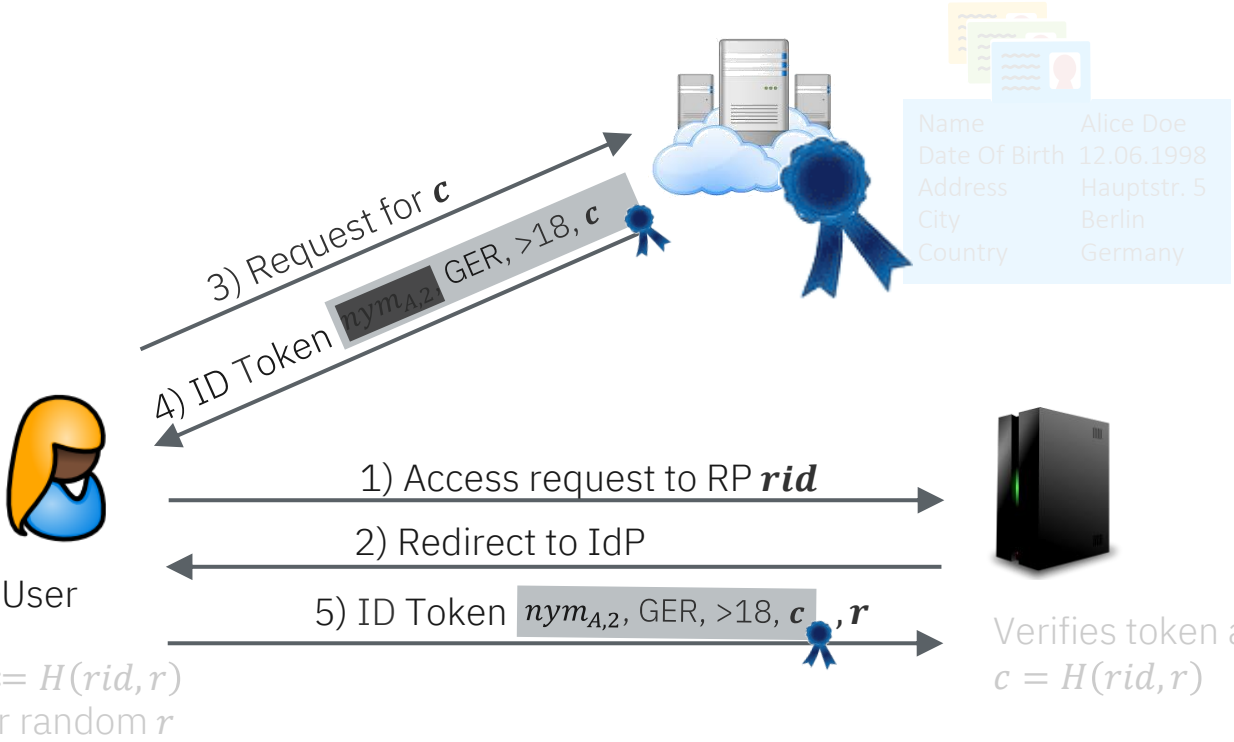
Verifies token and that
$c = H(rid, r)$

$c := H(rid, r)$
for random r

Properties	SSO
Usability	✓
Strong Authentication	✓
Selective Disclosure	✓
Unlinkability (RP)	✓
Unobservability (IdP)	✓

Single Sign-On | Are we done?

- No! RP Authentication is missing → only registered RPs must be allowed to use SSO service



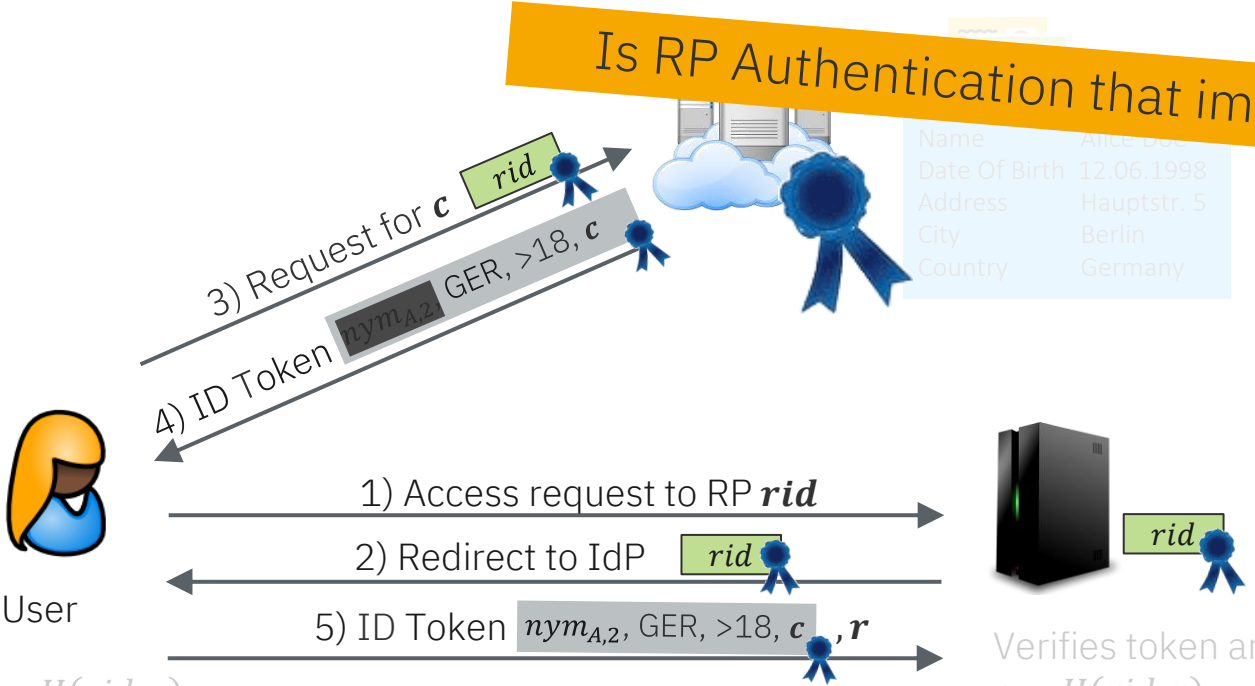
Properties	SSO
Usability	✓
Strong Authentication	✓
Selective Disclosure	✓
Unlinkability (RP)	✓
Unobservability (IdP)	✓
RP Authentication	✗

Single Sign-On | Are we done?

- No! RP Authentication is missing → only registered RPs must be allowed to use SSO service
- Easy to add – RP has membership certificate from IdP & authenticates with every request

Is RP Authentication that important?

→ But breaks privacy!

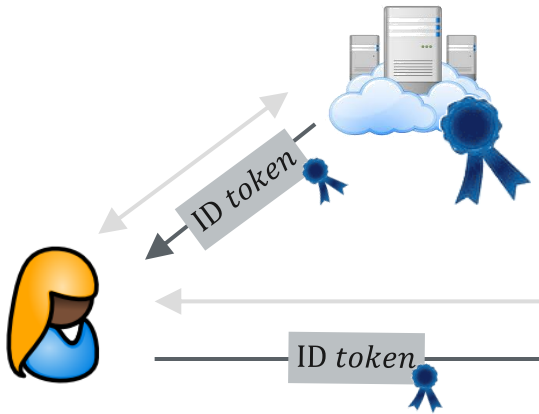


Properties	SSO
Usability	✓
Strong Authentication	✓
Selective Disclosure	✓
Unlinkability (RP)	✓
Unobservability (IdP)	⊘
RP Authentication	✓

Single Sign-On | Reality Check → Need for RP Authentication

Front Channel (aka Implicit Flo … Channel (aka Authorization Code Flow)

Implicit Flow is deprecated from OAuth 2.1
→ w/o Implicit Flow, no chance for privacy-preserving SSO



Specification(s)

OIDC ?

Draft: OAuth 2.1

Version 11: May '24

~~Implicit Flow~~

Auth. Code Flow

- RP Authentication by default
- Privacy/Unobservability impossible

"The OAuth 2.0 **Implicit grant is omitted from OAuth 2.1** as it was deprecated in [I-D.ietf-oauth-security-topics]."

"The [IdP] issuing access tokens to the client after successfully authenticating the [RP] and obtaining authorization."

eIDAS 2.0 §8:
[..], **relying parties** should provide the information necessary to allow for their identification and **authentication** towards the European Digital Identity Wallets

European Digital Identity Wallet

Pretty good – not ideal though, privacy is recommended but not required!

& unobservability added after open letter by privacy reseachers → with a caveat though

- eIDAS 2.0 published in December 2023:

§7: The technical framework of the European Digital

(a) **not allow providers** of electronic attestations of attributes or any other party, after the issuance of the attestation of attributes, to obtain data that allows **for tracking, linking, correlating** or otherwise obtain knowledge of transactions or user behaviour unless explicitly authorised by the user.

(b) **enable privacy preserving techniques** which ensure **unlinkability**, …

§9c: EDIWs should include a functionality to generate user chosen and managed **pseudonyms**, to authenticate when accessing online services

§29: The EDIW should technically enable the **selective disclosure** of attributes to relying parties.

Annex 11(c)
The use of the wallet [..] should not result in the processing of data **beyond what is necessary for the provision of wallet services**. To ensure privacy, EDIW providers should ensure **unobservability** by not collecting data and not having insight into the transactions of the users of the Wallet.

§8: [..], relying parties should provide the information necessary to allow for their identification and **authentication** towards the European Digital Identity Wallets

Our Work: Privacy-Preserving SSO with RP Authentication

- SSO with RP Authentication and
  - Unobservability: IdP doesn't learn rid
  - RP Binding (part of Strong Auth): Tokens are bound to rid
  - Unlinkability: IdP derives rid-specific pseudonym

Save The Implicit Flow? Enabling Privacy-Preserving RP Authentication in OpenID Connect

Maximillian Kroschewski, Anja Lehmann

PETS 2023

OPPID: Single Sign-On with Oblivious Pairwise Pseudonyms

Maximillian Kroschewski, Anja Lehmann, Cavit Özbay

work in progress, on ePrint soon

Properties	Our Work(s)
Usability	✓
Strong Authentication	✓
Selective Disclosure	✓
Unlinkability (RPs)	✓
Unobservability (IdP)	✓
RP Authentication	✓

Privacy-Preserving Single-Sign On with RP Authentication

Anonymous Credentials to the rescue → but for the RP!

Key pair $isk := (isk_{RP}, isk_\tau)$ $ipk := (ipk_{RP}, ipk_\tau)$

$cred := Sign(isk_{RP}, rid)$

signature scheme with efficient proofs

RP Registration:

IdP issues *anonymous credential* to RP on its rid

Privacy-Preserving SSO | User & RP Authentication

- Idea similar to [HSB20]: IdP signs committed rid
- But we use Pedersen commitment & NIZK proof to authenticate the hidden rid

- Requirements – IdP must:
  - Verify that request comes from registered RP
  - Bind token to the RP rid
  - Not learn RPs rid

3) Request + RP Auth $sid, uid, (c, \pi)$

4) ID Token sid, τ

Verify π w.r.t ipk_{RP}, sid, c

Compute ID token as

$$\tau := Sign(isk_\tau, (c, uid, sid))$$

standard signature

$(isk_{RP}, isk_\tau), (ipk_{RP}, ipk_\tau)$

$cred := Sign(isk_{RP}, rid)$

1) Access request to RP rid, c, o

2) RP Auth: sid, π

$c := Com(rid, o)$

for random o

Verify that $c = Com(rid, o)$

$$\pi := NIZK\left\{\begin{matrix}(rid, cred): Vf(ipk_{RP}, rid, cred) = 1 \\ \wedge\, c = Com(rid, o)\end{matrix}\right\}(sid)$$

Privacy-Preserving SSO | User & RP Authentication

- Final token should be self-contained & verifiable for (uid, rid, sid)

Verify π w.r.t ipk_{RP}, sid, c

Compute ID token as

$$\tau := Sign\big(isk_\tau, (c, uid, sid)\big)$$

standard signature

3) Request + RP Auth $sid, uid, (c, \pi)$

4) ID Token sid, τ

$(isk_{RP}, isk_\tau), (ipk_{RP}, ipk_\tau)$

$cred := Sign(isk_{RP}, rid)$

1) Access request to RP rid, c, o

2) RP Auth: sid, π

$c := Com(rid, o)$ for random o

5) ID Token $sid, uid, \tau_{fin} := (\tau, c, o)$

Verify that τ_{fin} is valid for (uid, rid, sid):

Parse $\tau_{fin} = (\tau, c, o)$

$Vf(ipk_\tau, (c, uid, sid), \tau) = 1$ and $c = Com(rid, o)$

Privacy-Preserving SSO | Security & Privacy

Only registered RPs can provide valid π
(Soundness of NIZK & unforgeability of Anon Cred) → RP Authentication

Verify π w.r.t ipk_{RP}, sid, c
Compute ID token as
$\tau := Sign(isk_\tau, (c, uid, sid))$

IdP learns nothing about rid due to hiding commitment & ZK property of π
→ RP Hiding / Unobservability

IdP blindly binds token to rid by signing commitment c → RP Binding

1) Access request to RP rid, c, o

2) RP Auth: sid, π

$c := Com(rid, o)$
for random o

5) ID Token $sid, uid, \tau_{fin} := (\tau, c, o)$

Verify that τ_{fin} is valid for (uid, rid, sid):
Parse $\tau_{fin} = (\tau, c, o)$
$Vf(ipk_\tau, (c, uid, sid), \tau) = 1$ and $c = Com(rid, o)$

Privacy-Preserving SSO | No Pseudonyms yet!

- Challenge: how can IdP compute RP-specific pseudonyms without learning rid ?

3) Request + RP Auth $sid, uid, (c, \pi)$

4) ID Token sid, τ

Verify π w.r.t ipk_{RP}, sid, c

Compute ID token as

$\tau := Sign(isk_\tau, (c, uid, sid))$

$$nym = F_k(uid, rid)$$

$cred := Sign(isk_{RP}, rid)$

1) Access request to RP rid, c, o

2) RP Auth: sid, π

$c := Com(rid, o)$ for random o

5) ID Token $sid, uid, \tau_{fin} := (\tau, c, o)$

Verify that τ_{fin} is valid for (uid, rid, sid):

Parse $\tau_{fin} = (\tau, c, o)$

$Vf(ipk_\tau, (c, uid, sid), \tau) = 1$ and $c = Com(rid, o)$

Privacy-Preserving SSO | Pseudonyms

Combining ideas from scope-exclusive pseudonyms & OPRFs

- Focus just on pseudonyms for now...
  - Unique per user & RP
  - Unlinkable across RPs
  - Blindly computable

3) Req $sid, uid, \overline{rid} := H(rid)^r$

4) ID Token $sid,$ τ

Blindly compute ID Token τ for sid, rid and

$$nym = F_k(uid, rid)$$

$$= \underbrace{H(rid)^{PRF(k,uid)}}$$

OPRF-ish: User sends $\overline{rid} := H(rid)^r$

$cred := Sign(isk_{RP}, rid)$

1) Access request to RP rid

2) RP Auth: sid, π

$\overline{rid} := H(rid)^r$

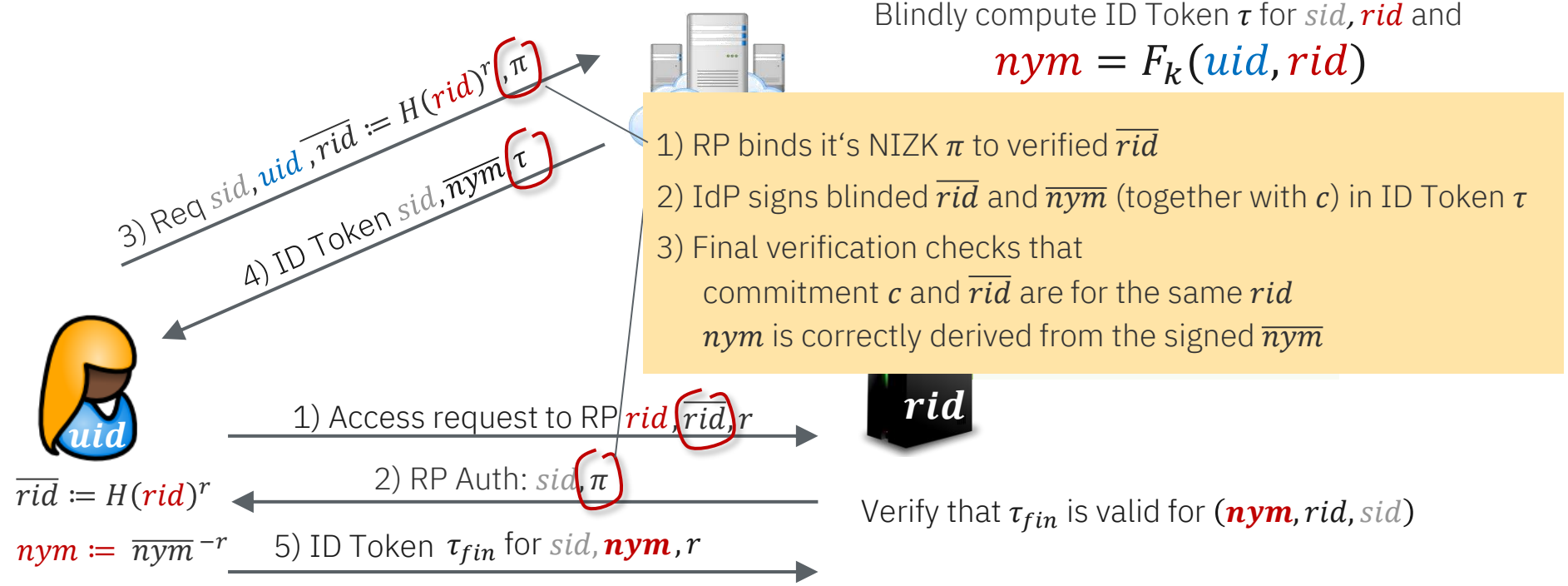
$nym := \overline{nym}^{-r}$

5) ID Token τ_{fin} for $sid, \mathbf{nym}, r$

Verify that τ_{fin} is valid for $(\mathbf{nym}, rid, sid)$

Privacy-Preserving SSO | Pseudonyms & RP Authentication

- How to ensure that pseudonym is computed for correct rid ?



Privacy-Preserving Single Sign-On | Summary

Properties	SSO
Usability	✓
Strong Authentication	✓
Selective Disclosure	✓
Unlinkability (RPs)	✓
Unobservability (IdP)	✓
RP Authentication	✓
Untraceability (RP & IdP)	✗

- Efficient protocol from simple building blocks
  - Standard signatures (→ RSA)
  - Signatures with efficient proofs (→PS)
  - Commitments (→ Pedersen)
  - Pseudonyms: DDH Group, (HMAC)-SHA-256
  - Running time of 2-20ms per party

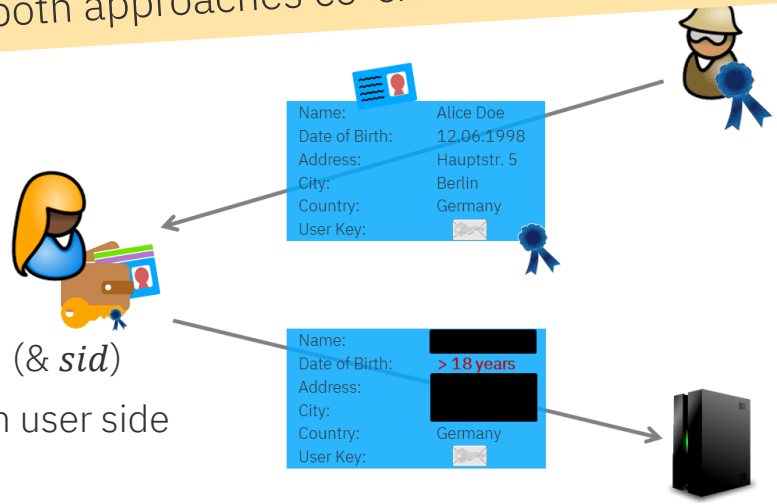
- Limitation: No Privacy against colluding IdP & RP!
  - Deterministic pseudonyms, linkage via timing information (& sid)
  - Inherent in solutions with single IdP and no keys/creds on user side

Privacy-Preserving Single Sign-On | Comparison

Properties	SSO	Anon Cred
Usability	✓	✗
Strong Authentication	✓	✓
Selective Disclosure	✓	✓
Unlinkability (RPs)	✓	✓
Unobservability (IdP)	✓	✓
RP Authentication	✓	Out of scope
Untraceability (RP & IdP)	✗	✓

Are we „privacy-washing“ an inherently bad solution?

- No – open for discussion ;)
- We need usable solutions → convenience is key
- Ideally both approaches co-exist: user‘s choice



- Limitation: No Privacy against colluding IdP & RP!
  - Deterministic pseudonyms, linkage via timing information (& sid)
  - Inherent in solutions with single IdP and no keys/creds on user side