Sichere und interoperable Protokolle für Digitale Identitäten

Dr. Daniel Fett
SPRIND

Architekturentwurf EUDI-Wallet

Entwurf zur deutschen Implementierung des europäischen Wallets

- ➔ Teil des ergebnisoffenen, öffentlichen Konsultationsprozesses
- ➔ Identifizierung der besten Architektur zur Umsetzung der neuen eIDAS-2-Verordnung
- ➔ Sicherstellung der europäischen Interoperabilität
- ➔ Entwicklung einer wallet-basierten leichtgewichtigen eID-Lösung

https://gitlab.opencode.de/bmi/eudi-wallet/eidas-2.0-architekturkonzept-v1

Protokolle und Formate im aktuellen Entwurf

Credential-Formate

SD-JWT VC (IETF)

W3C Verifiable Credentials

mdoc (ISO)

Übertragungsprotokolle

OpenID for Verifiable Credentials

ISO-18013 RestAPI

Protokolle und Formate im aktuellen Entwurf

Credential-Formate

SD-JWT VC (IETF)

W3C Verifiable Credentials

mdoc (ISO)

Übertragungsprotokolle

OpenID for Verifiable Credentials

ISO-18013 RestAPI

OpenID for Verifiable Credentials

- ★ Familie von Protokollen
- ★ Ausstellung und Präsentation von Credentials aller Formate
- ★ Basierend auf OAuth 2.0
  - Standard für Autorisierung im Web
  - Weit verbreitet und in zahlreichen Anwendungen eingesetzt
  - **Sicherheit gut verstanden & analysiert**
- ★ Entwickelt in der OpenID Foundation
  - Expertise rund um OpenID Connect und mehr
  - Offener, für alle zugänglicher Standardisierungsprozess
- ★ Umfangreiche, detaillierte Sicherheitsanalyse durch Universität Stuttgart

https://openid.net/formal-security-analysis-openid-verifiable-credentials/

SD-JWT und SD-JWT VC

- ★ SD-JWT: Format für Selective Disclosure mit JWTs
  - Einfaches Format
  - Universell nutzbar
  - Referenzimplementierung in der Open Wallet Foundation und zahlreiche unabhängige Implementierungen
- ★ SD-JWT VC
  - Regeln für Verifiable Credentials mit SD-JWT
  - Einfaches JSON-Format (kein JSON-LD)
  - Bewährte JWT-Ideen
- ★ Entwickelt als Internetstandard in der IETF

https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/

Sicherheits- und Datenschutzfunktionen

Credential-Formate

SD-JWT VC (IETF)

W3C Verifiable Credentials

mdoc (ISO)

Übertragungsprotokolle

OpenID for Verifiable Credentials

ISO-18013 RestAPI

Selective Disclosure

Unlinkability

(und noch viele, viele weitere…)

Sicherheits- und Datenschutzfunktionen

Credential-Formate

SD-JWT VC (IETF)

W3C Verifiable Credentials

mdoc (ISO)

Übertragungsprotokolle

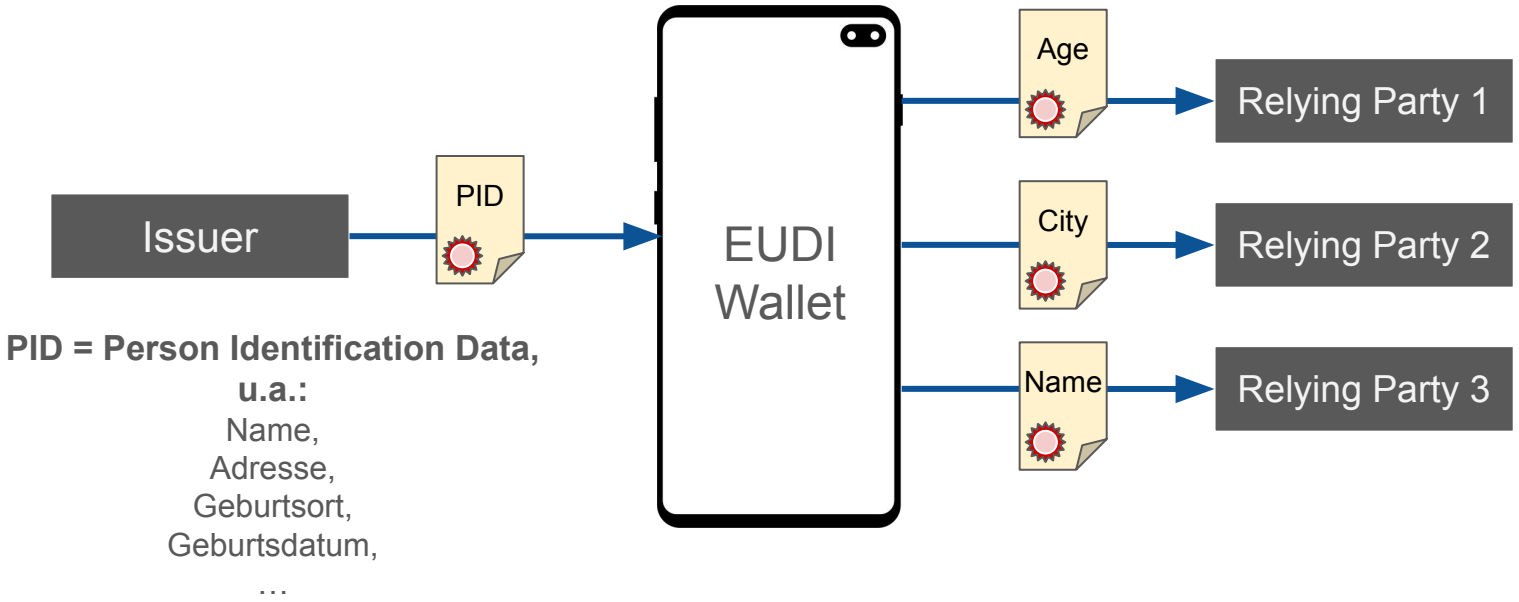
OpenID for Verifiable Credentials

ISO-18013 RestAPI

Selective Disclosure

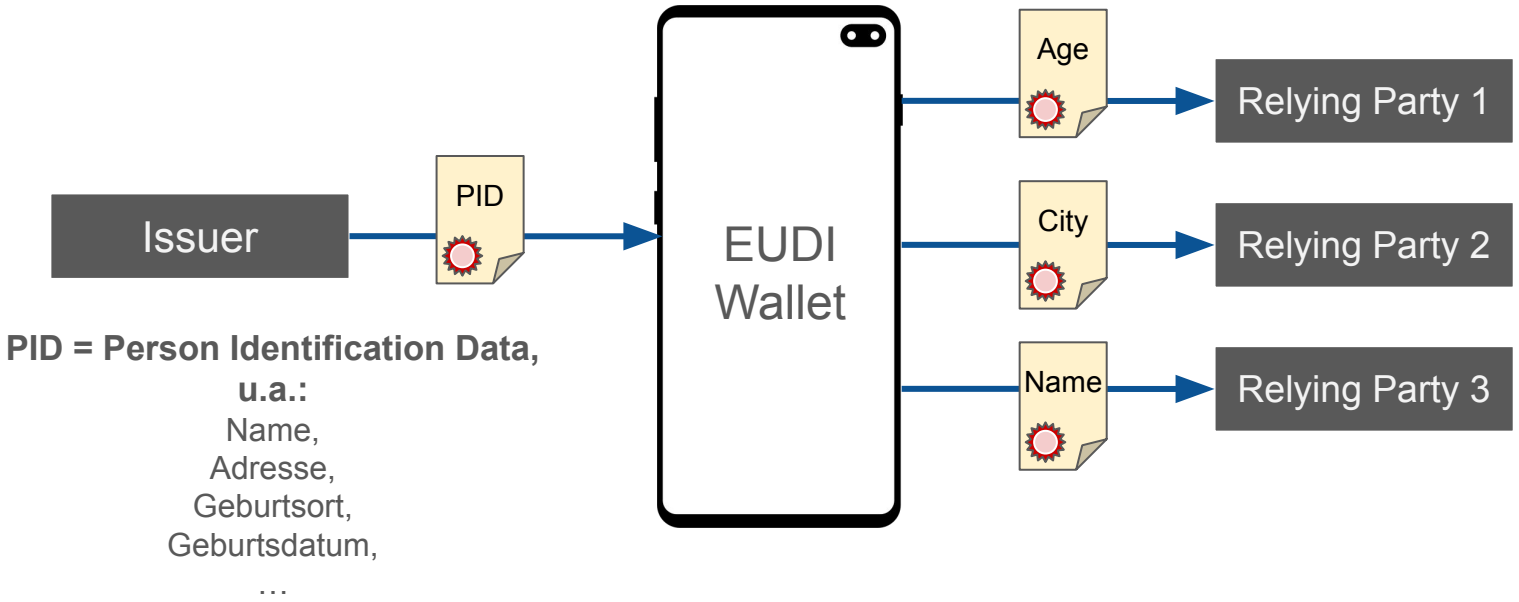
Unlinkability

Selective Disclosure



PID = Person Identification Data, u.a.:
Name,
Adresse,
Geburtsort,
Geburtsdatum,
…

Selective Disclosure



PID = Person Identification Data, u.a.:
Name,
Adresse,
Geburtsort,
Geburtsdatum,
…

Herausforderung:
Signatur des Ausstellers muss auch bei teilweiser Offenlegung der PID-Daten gültig sein.

Selective Disclosure in 5 einfachen Schritten

Schritt 1: Benutzerdaten vorbereiten


```
{
 "iss": "https://example.com",
 "vct": "IdentityCredential",
 "cnf": {"jwk": {"kty": "RSA","n": "0vx....Kgw","e": "AQAB" } },
 "given_name": "Max",
 "family_name": "Mustermann",
 "email": "mustermann@example.com",
 "address": {
   "street_address": "Musterstr. 23",
   "locality": "Berlin",
   "country": "DE"
 }
}
```

Selective Disclosure in 5 einfachen Schritten

Schritt 2: Erstellen von *Disclosures*

```
{
 "iss": "https://example.com",
 "vct": "IdentityCredential",
 "cnf": {"jwk": {"kty": "RSA","n": "0vx....Kgw","e": "AQAB" } },
 "given_name": "Max", ····· ["GO0r26nO-iW50ZcAoOilFw", "given_name", "Max"]
 "family_name": "Mustermann",····· ["cSlbR135iONjhsouMxrjjg", "family_name", "Mustermann"]
 "email": "mustermann@example.com",····· ["oHDt43Vwuhpo8mzaprgCcw", "email", "mustermann@example.com"]
 "address": {
   "street_address": "Musterstr. 23",····· ["rGcOKtY6WmflywTTKEWIEQ", "street_address", "Musterstr. 23"]
   "locality": "Berlin",····· ["pGQMQx-2tH2XwC_eQCFn4g", "locality", "Berlin"]
   "country": "DE"    ····· ["TI15M8G5UIxPiWNZ-VLYBA", "country", "DE"]
 }
}
```

salt claim name claim value

Selective Disclosure in 5 einfachen Schritten

Schritt 3: Disclosures hashen und Originalwerte ersetzen

```
{
 "iss": "https://example.com",
 "vct": "IdentityCredential",
 "cnf": {"jwk": {"kty": "RSA","n": "0vx....Kgw","e": "AQAB" } },
 "_sd": [ "EW1oOegqa5mGcbytT5S-kAubcEjYEUwRkXlu2vC5l2O",          ← ["GOOr26nO-iW50ZcAoOilFw", "given_name", "Max"]
          "FEx-ITHt41I8_cnOSS-hvoLneX_RGlJo_8o2xRNhfdk",          ← ["cSlbR135i0NjhsouMxrjjg", "family_name", "Mustermann"]
          "igg7H5fn2eBEMIEkE5Ckbm23QuwDJlTYoKRip08dYIc" ],         ← ["oHDt43Vwuhpo8mzaprgCcw", "email", "mustermann@example.com"]
 "address": {
   "_sd": [ "gqB5kmAwyry88aHjaAeO-USX6JOMaojukKsheo38OOc",        ← ["rGcOKtY6WmflywTTKEWIEQ", "street_address", "Musterstr. 23"]
            "w8InvxsPXdKoowuVpyBMgl1b9_R2b6Xpa3OYOIjgQro",        ← ["pGQMQx-2tH2XwC_eQCFn4g", "locality", "Berlin"]
            "vOnlYtcjr872fP3Wa75Ozl7c-6_MOVdIUNtwLKKxZw0" ]       ← ["TI15M8G5UIxPiWNZ-VLYBA", "country", "DE"]
 }
}
```

Selective Disclosure in 5 einfachen Schritten

Schritt 4: Signieren und als JSON Web Token (JWT) verpacken

```
{
  "iss": "https://example.com",
```

```
eyJhbGciOiAiUlMyNTYiLCAia2lkIjogImNBRUlVcUowY21MekQxa3pHemhlaUJhZzBZ
UkF6VmRsZnhOMjgwTmdIYUEifQ.eyJpc3MiOiAiaHR0cHM6Ly9leGFtcGxlLmNvbS9pc
3N1ZXIiLCAiY25mIjogeyJqd2siOiB7Imt0eSI6ICJSU0EiLCAibiI6ICIwdng3YWdvZ
WJHY1FTdS4uLi4tY3NGQ3VyLWtFZ1U4YXdhcEp6S25xREtndyIsICJlIjogIkFRQUIif
X0sICJ0eXBlIjogIklkZW50aXR5Q3JlZGVudGlhbCIsICJjcmVkZW50aWFsU3ViamVjd
CI6IHsiX3NkIjogWyJFVzFvMGVncWE1bUdjYnl0VDVTLWtBdWJjRWpZRVV3UmtYbHUyd
kM1bDIwIiwgIkZFeC1JVEh0NDFJOF9jbjBTUy1odm9MbmVYX1JHbEpvXzhvMnhSTmhmZ
GsiLCAiUXhKViOyVjFIOG1jbHRSNnZWQzRtM3JlVTVhTkg5d2RKejJVZG1Sb0kxRSIsI
CJhdFVuMVRZd1JBbDRHUTdQZUV0WGFNdzJmNHVJVGlKclgOODV3TTh2NjdFIiwgImZUT
XczdmtrRUx3TDFYTnVZSzhIN3pCS0NIdV91aWY2MFNsRzFweVhJVVEiLCAiaWdnNOg1Z
m4yZUJFTUlFaOU1Q2tibTIzUXV3REpsVFlvS1JpcDA4ZFlJYyIsICJ0cFV0bDcwaHBVX
3hucnZaaTBHaEdvUlIxam1OMXpZZ3Z2NUlZMEF4N0tjIl0sICJhZGRyZXNzIjogeyJfc
2QiOiBbImdxQjVrbUF3eXJ5ODhhSGphQWVPLVVTWDZKT01hb2p1a0tzaGVvMzhPMGMiL
CAidk9ubFlOY2pyODcyZlAzV2E3NU96bDdjLTZfTU9WZElVTnR3TEtLeFp3MCIsICJ3O
EludnhzUFhkS29vd3VWcHlCTWdsMWI5X1IyYjZYcGEzT1lPSWpnUXJvIl19fSwgImlhd
CI6IDE1MTYyMzkwMjIsICJleHAiOiAxNTE2MjQ3MDIyLCAic2RfZGlnZXN0X2Rlcml2Y
XRpb25fYWxnIjogInNoYS0yNTYifQ.1UHEPtLLUXOT51jH3gg-3C-ZidWzsB9Un-VxmM
VdQtTbLLhwDTB6HJtt15p43yCXTzdpiZxtDI6fr07TpODy_Umg3Q5_FxFj4WHnsVuVzu
ASU8cFlGPi6xgH9D3w1G2hqepBS8DyQ5bA_p5kN_tKJVoP1xWhcQujRJ8kkEKQsRia4F
hrBldl8f41wgu_ipPqh1Ix4BVI7GJClZNx94nWPT7JUFkI6Y6JkahLf3S6gBOMxtmLAe
YOqkuz8VeOZNfl_CDog55kVTkArorfoL6D6TEjI__-w6YyUOPnIRJXJOwrYfoyhNl8LK
AP38QYMpdR7z_rsvHpQHzFAPTmevnHDg
```

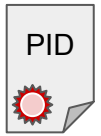
```
["GOOr26nO-iW50ZcAoOilFw", "given_name", "Max"]
["cSlbR135iONjhsouMxrjjg", "family_name", "Mustermann"]
["oHDt43Vwuhpo8mzaprgCcw", "email", "mustermann@example.com"]

["rGcOKtY6WmflywTTKEWIEQ", "street_address", "Musterstr. 23"]
["pGQMQx-2tH2XwC_eQCFn4g", "locality", "Berlin"]
["TI15M8G5UIxPiWNZ-VLYBA", "country", "DE"]
```

Selective Disclosure in 5 einfachen Schritten

Schritt 5: Disclosures base64-kodieren und anhängen

```
{
  "iss": "https://example.com",
eyJhbGciOiAiUlMyNTYiLCAia2lkIjogImNBRUlVcUowY21MekQxa3pHemhlaUJhZzBZ
UkF6VmRsZnhOMjgwTmdIYUEifQ.eyJpc3MiOiAiaHR0cHM6Ly9leGFtcGxlLmNvbS9pc
3N1ZXIiLCAiY25mIjogeyJqd2siOiB7Imt0eSI6ICJSU0EiLCAibiI6ICIwdng3YWdvZ
WJHY1FTdS4uLi4tY3NGQ3VyLWtFZ1U4YXdhcEp6S25xREtndyIsICJlIjogIkFRQUIif
X0sICJ0eXBlIjogIklkZW50aXR5Q3JlZGVudGlhbCIsICJjcmVkZW50aWFsU3ViamVjd
CI6IHsiX3NkIjogWyJFVzFvMGVncWE1bUdjYnl0VDVTLWtBdWJjRWpZRVV3UmtYbHUyd
kM1bDIwIiwgIkZFeC1JVEh0NDFJOF9jbjBTUy1odm9MbmVYX1JHbEpvXzhvMnhSTmhmZ
GsiLCAiUXhKViOyVjFIOG1jbHRSNnZWQzRtM3JlVTVhTkg5d2RKejJVZG1SbOkxRSIsI
CJhdFVuMVRZd1JBbDRHUTdQZUVOWGFNdzJmNHVJVGlKclgOODV3TTh2NjdFIiwgImZUT
XczdmtrRUx3TDFYTnVZSzhIN3pCS0NIdV91aWY2MFNsRzFweVhJVVEiLCAiaWdnNOg1Z
m4yZUJFTUlFaOU1Q2tibTIzUXV3REpsVFlvS1JpcDA4ZFlJYyIsICJOcFVObDcwaHBVX
3hucnZaaTBHaEdvUlIxam1OMXpZZ3Z2NUlZMEF4NOtjIlOsICJhZGRyZXNzIjogeyJfc
2QiOiBbImdxQjVrbUF3eXJ5ODhhSGphQWVPLVVTWDZKT01hb2p1aOtzaGVvMzhPMGMiL
CAidk9ubFlOY2pyODcyZlAzV2E3NU96bDdjLTZfTU9WZElVTnR3TEtLeFp3MCIsICJ3O
EludnhzUFhkS29vd3VWcHlCTWdsMWI5X1IyYjZYcGEzT1lPSWpnUXJvIl19fSwgImlhd
CI6IDE1MTYyMzkwMjIsICJleHAiOiAxNTE2MjQ3MDIyLCAic2RfZGlnZXNOX2Rlcml2Y
XRpb25fYWxnIjogInNoYS0yNTYifQ.1UHEPtLLUXOT51jH3gg-3C-ZidWzsB9Un-VxmM
VdQtTbLLhwDTB6HJtt15p43yCXTzdpiZxtDI6fr07TpODy_Umg3Q5_FxFj4WHnsVuVzu
ASU8cFlGPi6xgH9D3w1G2hqepBS8DyQ5bA_p5kN_tKJVoP1xWhcQujRJ8kkEKQsRia4F
hrBldl8f41wgu_ipPqh1Ix4BVI7GJClZNx94nWPT7JUFkI6Y6JkahLf3S6gBOMxtmLAe
YOqkuz8VeOZNfl_CDog55kVTkArorfoL6D6TEjI__-w6YyUOPnIRJXJOwrYfoyhNl8LK
AP38QYMpdR7z_rsvHpQHzFAPTmevnHDg
```

```
~WyJHTzByMjZuTy1pVzUwWmNBb09pbEZ3IiwgImdpdmVuX25hbWUiLCAiTWF4Il0
~WyJjU2xiUjEzNWkwTmpoc291TXhyampnIiwgImZhbWlseV9uYW1lIiwgIk11c3R
lcm1hbm4iXQ
~WyJvSERONDNWd3VocG84bXphcHJnQ2N3IiwgImVtYWlsIiwgIm11c3Rlcm1hbm5
AZXhhbXBsZS5jb2OiXQ
~WyJyR2MwS3RZNldtZmx5d1RUS0VXSUVRIiwgInNOcmVldF9hZGRyZXNzIiwgIk1
1c3RlcnNOci4gMjMiXQ
~WyJwR1FNUXgtMnRIMlh3Q19lUUNGbjRnIiwgImxvY2FsaXR5IiwgIkJlcmxpbiJ
d
~WyJUSTE1TThHNVVJeFBpV05aLVZMWUJBIiwgImNvdW50cnkiLCAiREUiXQ
```



→ Done!

Sicherheits- und Datenschutzfunktionen

Credential-Formate

SD-JWT VC (IETF)

W3C Verifiable Credentials

mdoc (ISO)

Übertragungsprotokolle

OpenID for Verifiable Credentials

ISO-18013 RestAPI

Selective Disclosure

Unlinkability

Sicherheits- und Datenschutzfunktionen

Credential-Formate

SD-JWT VC (IETF)

W3C Verifiable Credentials

mdoc (ISO)

Übertragungsprotokolle

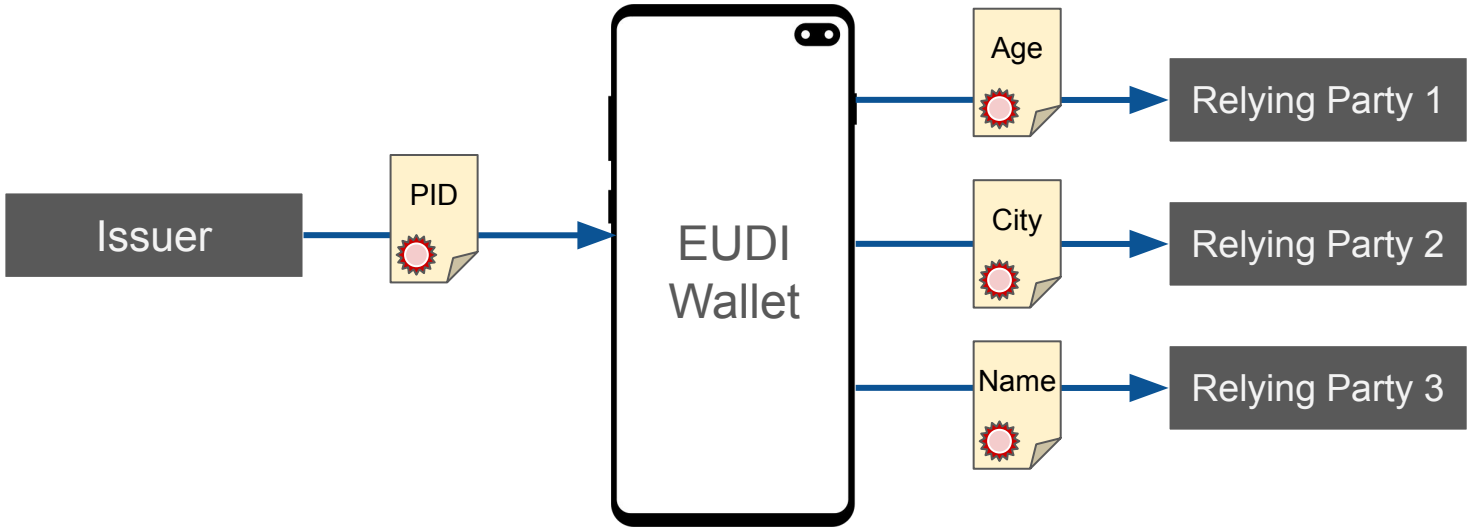
OpenID for Verifiable Credentials

ISO-18013 RestAPI

Selective Disclosure

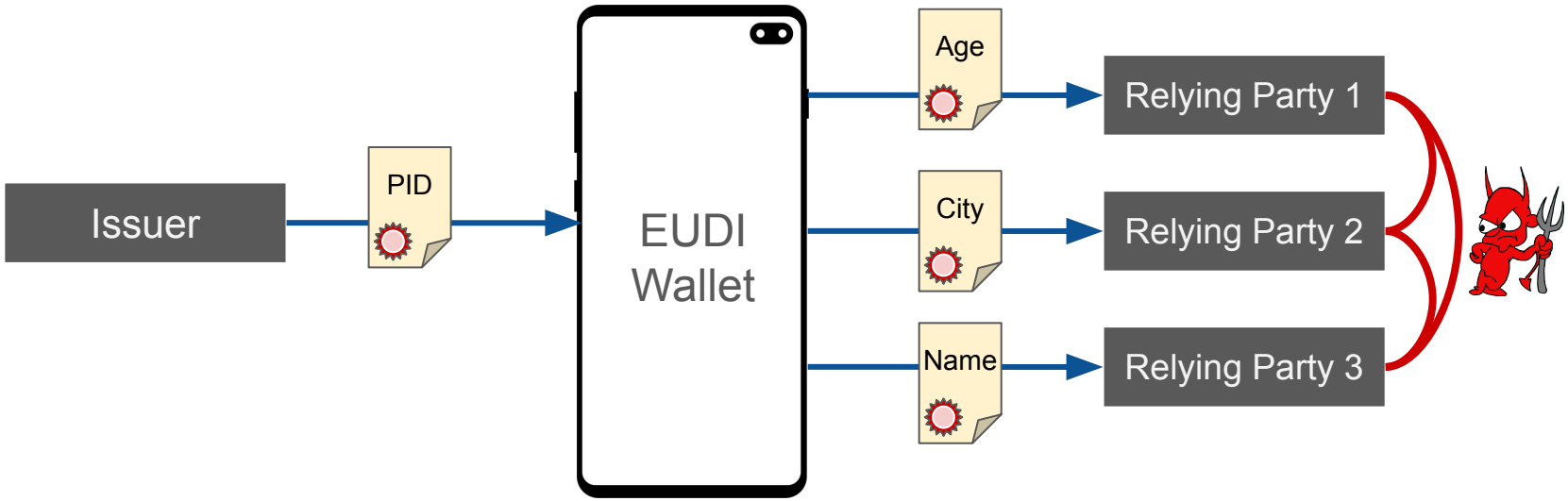
Unlinkability

Unlinkability?



PID = Person Identification Data

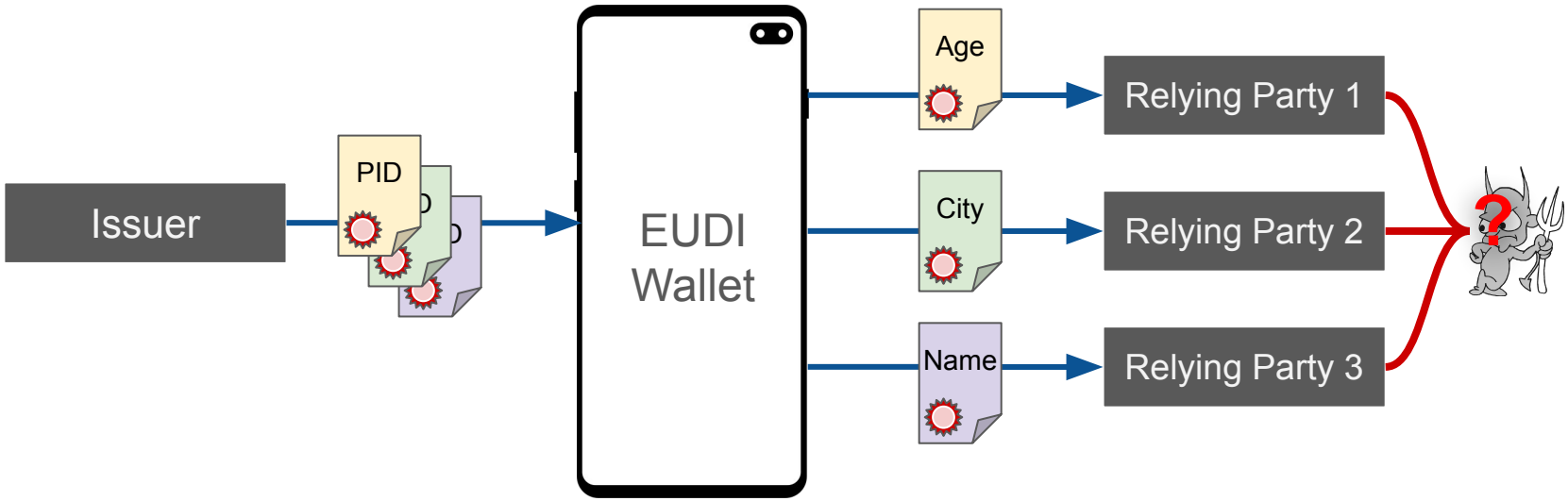
Unlinkability?



Problem:
Credential enthält — trotz Selective Disclosure — korrelierbare Werte: Nonces (Zufallszahlen), Hashes, Keys, …

PID = Person Identification Data

Batch-Issuance



Lösung:
Ausstellung von Batch-Credentials - gleiche Daten, frische Keys & Nonces.

PID = Person Identification Data

Sicherheits- und Datenschutzfunktionen

Credential-Formate

SD-JWT VC (IETF)

W3C Verifiable Credentials

mdoc (ISO)

Übertragungsprotokolle

OpenID for Verifiable Credentials

ISO-18013 RestAPI

Selective Disclosure

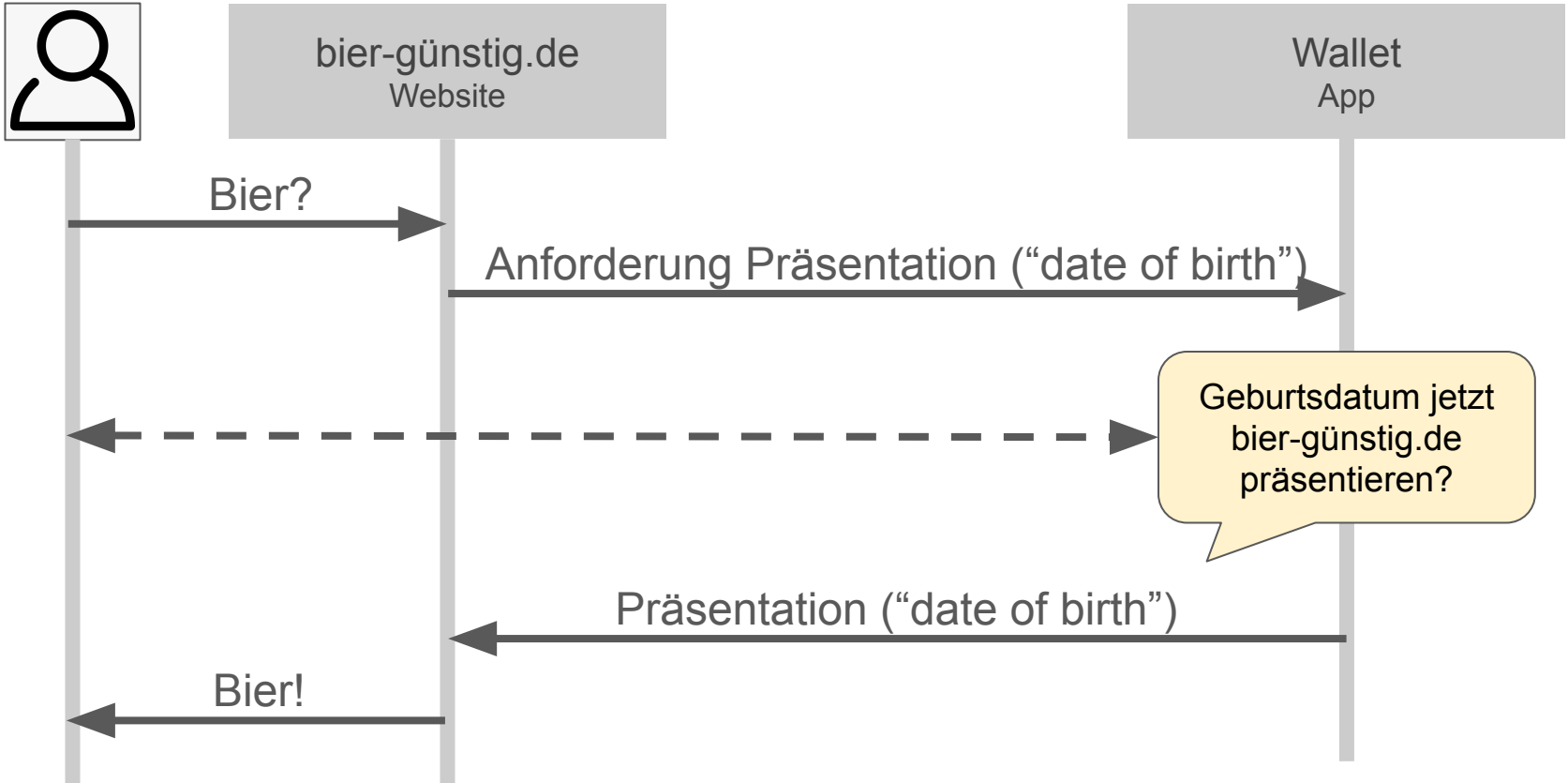
Unlinkability

(und noch viele, viele weitere…)

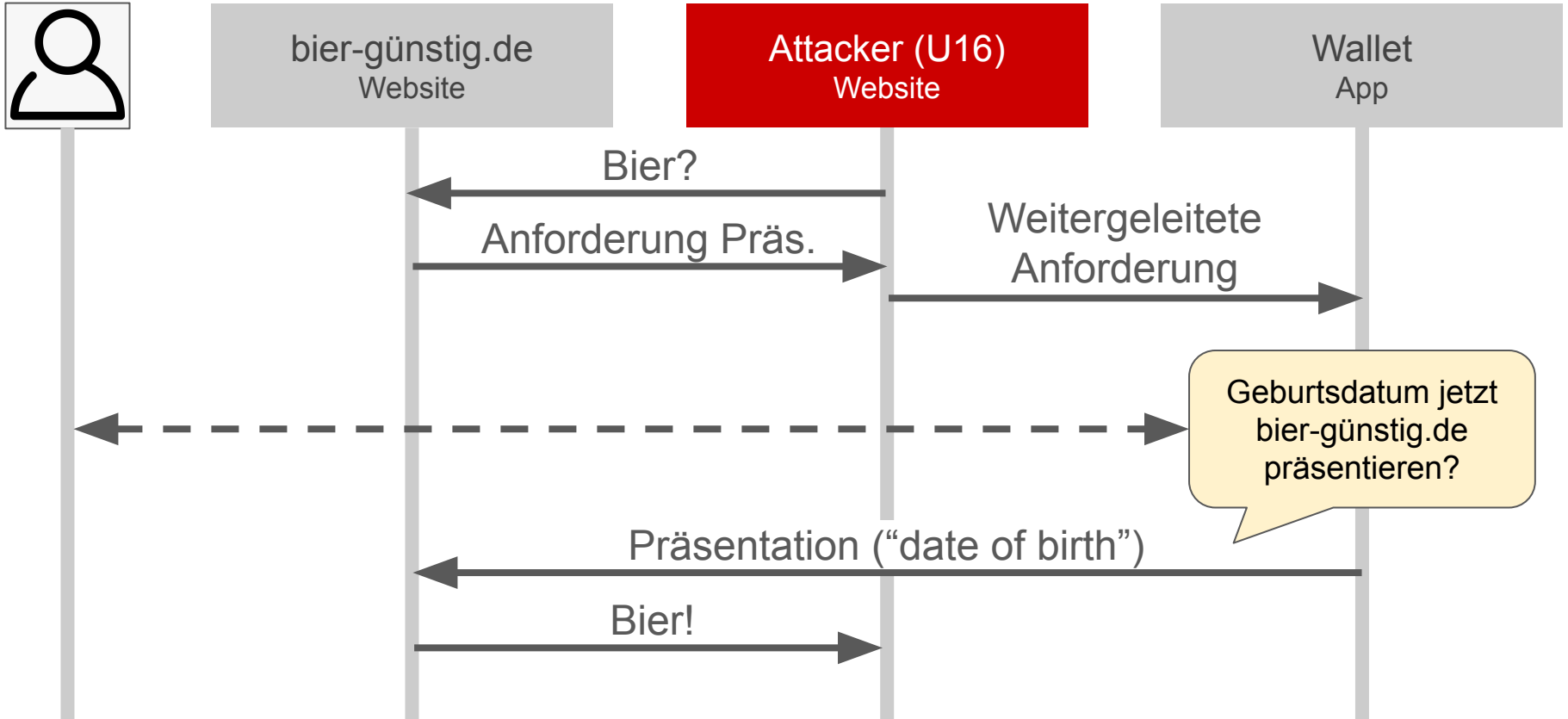
Vielen Dank!

Backup-Slides

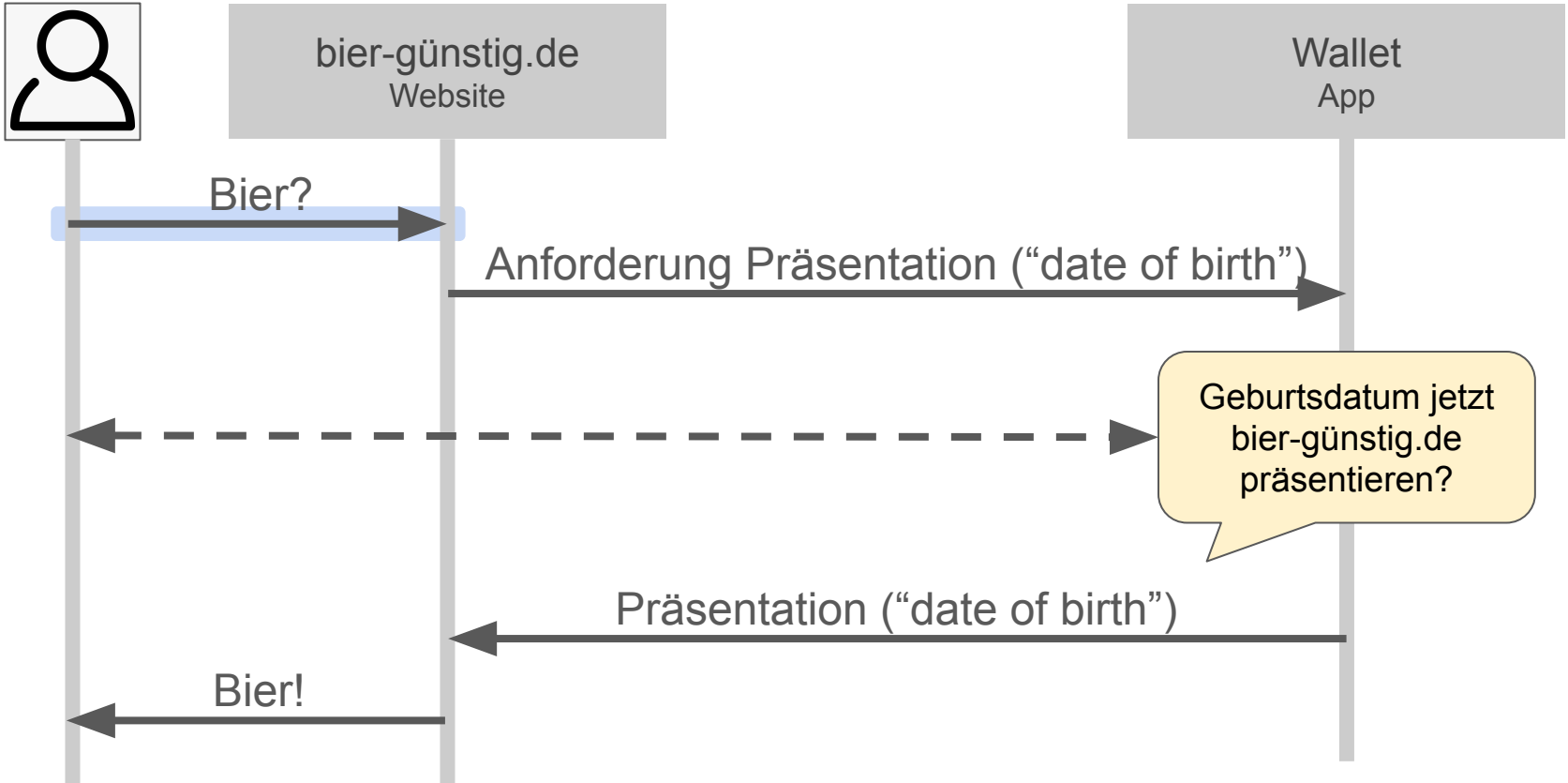
Session Integrity



Session Integrity — Attacker in the Middle



Lösung: Bindung an den Browser



Wie stellen wir Sicherheit her?

- Sicherheitsanalyse von Protokollen
- Sicherheitsanalyse von Cross-Device Flows
- “Best Current Practice”-Dokumente
- Batch Issuance