TeleTrusT Information Security Professional

TeleTrusT Pioneers in IT security.

T.I.S.P. Community Meeting 2019

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Berlin, 05. - 06.11.2019

Schön Sie kennenzulernen … Sichere Identitätsfeststellung in digitalen Endkundenszenarien mit OpenID Connect

Dr. Torsten Lodderstedt, yes.com

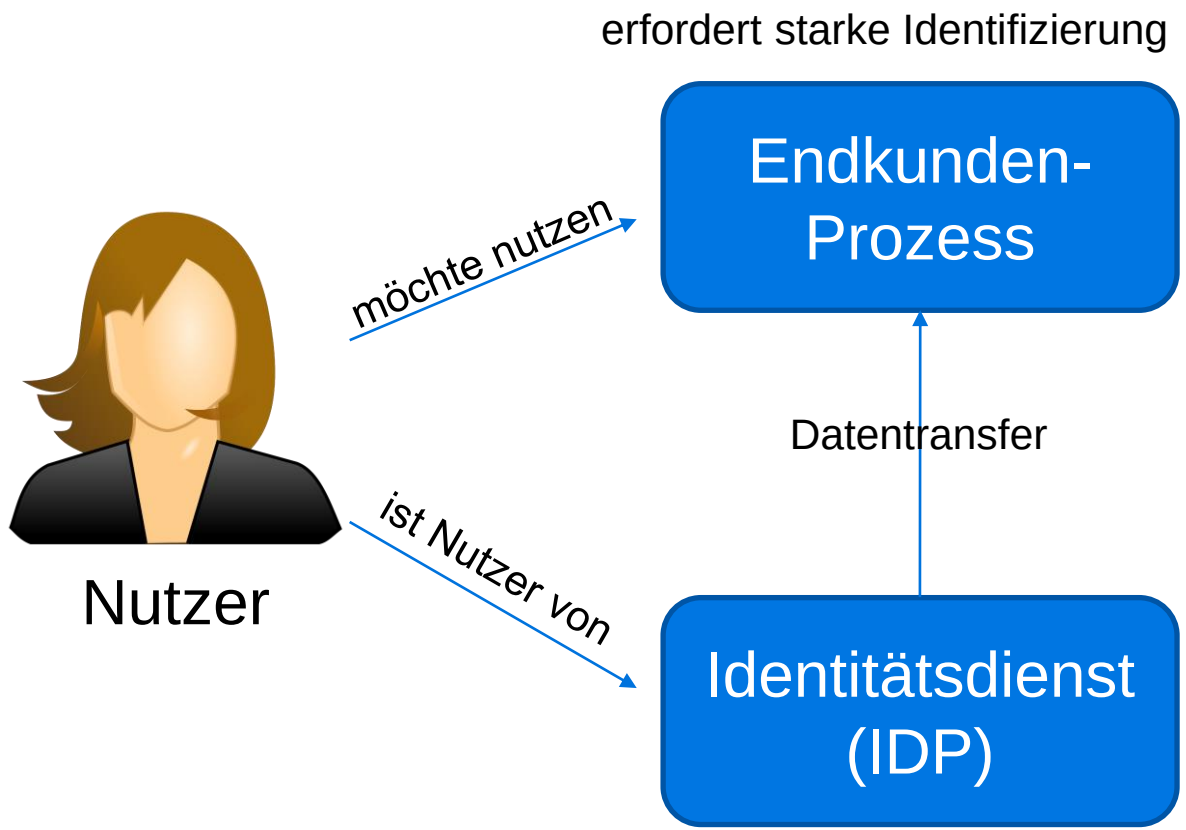
Herausforderung

- Viele digitale Prozesse mit Endkunden verlangen eine starke Identifizierung:
  - Geldwäschegesetz
  - Telekommunikationsgesetz
  - StGB §203, …
- Weitere gute Gründe: Betrugsbekämpfung & Risikominimierung
- Vergleichbares gilt im eGovernment-Bereich

Bisherige Lösungen

- Prüfung am Schalter
- PostIdent
- Video-Identifikation

Alternative: Identitätsdienste!



- Vertraut IDP
- Profitiert von einfachem Onboarding

- Authentifizierung Nutzer
- Einholen Zustimmung zum Datentransfer
- Verantwortet Datenqualität

Wo werden IDPs heute eingesetzt?

- Weit verbreitet in Szenarien mit relativ niedrigen Sicherheitsanforderungen
  - Onboarding für Shops, News-Portale, Developer-Portale
  - Typische IDPs: Google, Facebook, Twitter, LinkedIn, github
- Nutzen:
  - schnelles und unkompliziertes Onboarding
  - kein neuer Account erforderlich

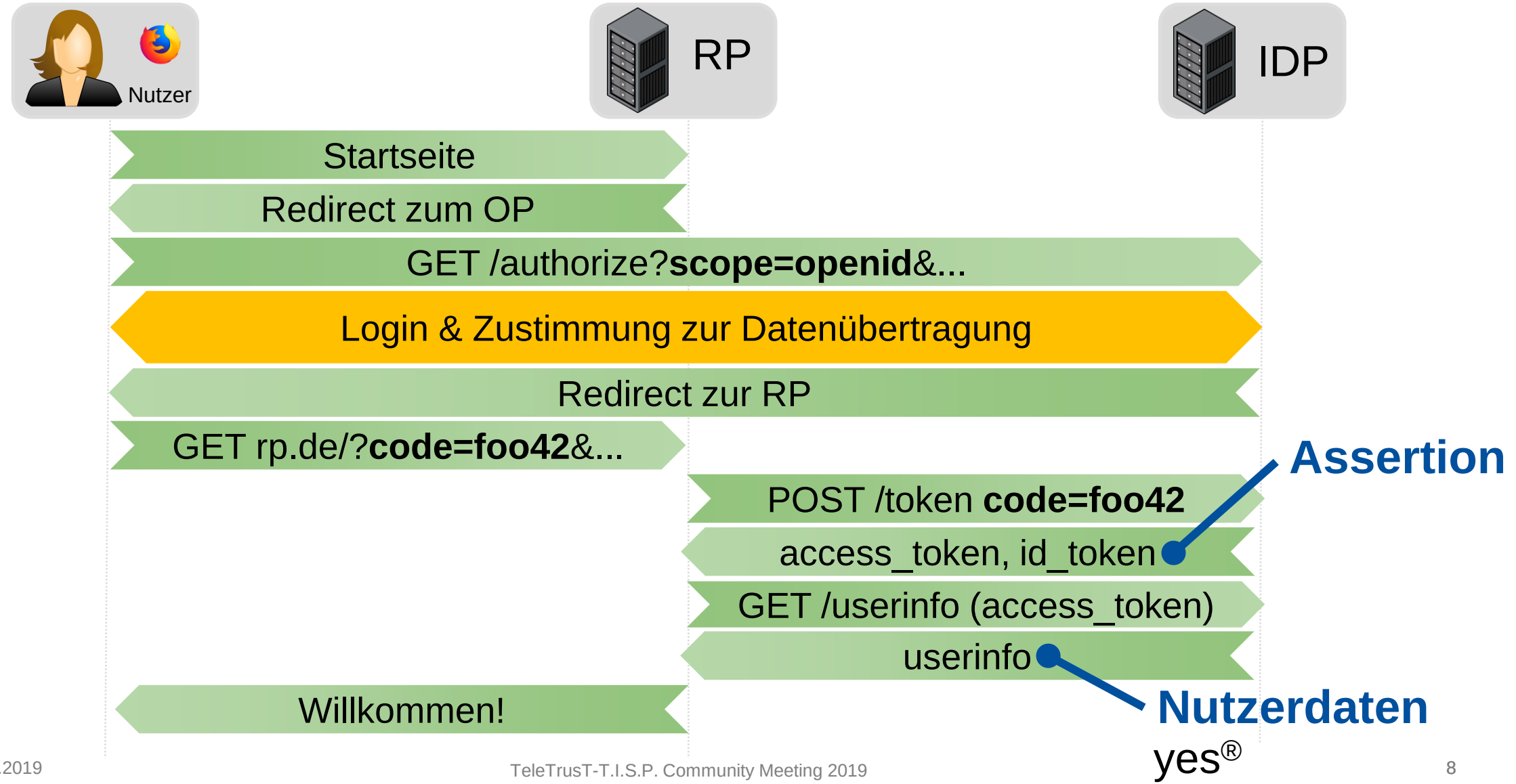
Technologie

- Industriestandard **OpenID Connect**
- Erweiterung von OAuth 2.0 (IETF) für Identity Providing
- Offener Standard der OpenID Foundation
- Aufbauend auf Erfahrungen von OpenID 2.0 und SAML

Starke Identifizierung und OpenID Connect?

- OpenID Connect wird in zunehmenden Maße auch für starke Identifizierung eingesetzt
- Einfach zu nutzen, bekannt und sicher (!)
- Beispiele: Mobile Connect, id4me, netid, Verimi, yes®, AusweisIDent

OpenID Connect: Ablauf



yes®

ID Token

Digital signierte Identitätsbestätigung (Assertion) als JSON Web Token (RFC 7519)

```
{
    "iss": "https://server.example.com",
    "sub": "24400320",
    "aud": "s6BhdRkqt3",
    "nonce": "n-0S6_WzA2Mj",
    "exp": 1311281970,
    "iat": 1311280970,
    "auth_time": 1311280969,
    "acr": "urn:mace:incommon:iap:silver"
}
```

UserInfo Response

JSON-formatierte Nutzerdaten (optional signiert und verschlüsselt)

```
HTTP/1.1 200 OK
Content-Type: application/json
{
    "sub": "24400320",
    "given_name": "Mustermann",
    "family_name": "Max",
    "email": "max@mustermann.de",
    "phone_number": "+49 (30) 123-4567",
    "address": {
        "street_address": "An der Sanddüne 22",
        "locality": "Musterstadt",
        "postal_code": "12344",
        "country": "DE"
    }
}
```

Nutzen

- Einfache und bewährte Schnittstelle
- Universelle Lösung: unterstützt Web, Mobile und APIs (durch Integration mit OAuth)
- Sicherheit ist systematisch untersucht und wissenschaftlich nachgewiesen

Starke Identifizierung braucht mehr

- Multi-Faktor-Authentifizierung
- Hohes Sicherheitsniveau der Datenübertragung
- Metadaten:
  - ursprünglicher Prüfprozess
  - verwendete Identitätsnachweise (z.B. Personalausweis)

Multi-Faktor Authentifizierung

- Moderne MFA-Verfahren sehr gut integrierbar (Redirect)
- Beispiel: Fido/WebAuthn, Authentifizierungs-Apps
- RP kann Authentifizierungsniveau anfordern und bekommt erreichtes Niveau vom IDP bestätigt

Sicherheitsniveau bei der Datenübertragung

- Mutual TLS für gegenseitige Authentifizierung sowie Schutz von Integrität und Vertraulichkeit
- Ende-zu-Ende Signierung und Verschlüsselung auf Anwendungsebene möglich
- Alle Interaktionen sind gegen Replay geschützt
  - PKCE, Sender Constrained Access Tokens
- OpenID Foundation publiziert FAPI Security Profiles

OpenID Connect for Identity Assurance

- Erweiterung für OpenID Connect
- Erlaubt Bereitstellung von verifizierten Daten zusammen mit detaillierten Metadaten zur Verifikation (was, wann, wie, welche Regeln, welche Nachweise)
- RP kann Abbildung auf eigenen Rechtsraum vornehmen und die (digital signierten) Daten zu Audit-Zwecken ablegen

Beispiel

- *trust_framework*: Prozess/Gesetz
- *evidence*: Identitätsnachweis, Prüfmethode
- *claims*: geprüfte Daten

```
{
  "verified_claims": {
    "verification": {
      "trust_framework": "de_aml",
      "time": "2016-04-23T18:25:43.511+01",
      "evidence": [
        {
          "type": "id_document",
          "method": "pipp",
          "document": {
            "type": "idcard",
            "issuer": {
              "name": "Stadt Musterstadt",
              "country": "DE"
            },
            "number": "53554GJM4",
            "date_of_expiry": "2022-04-22"
          }
        }
      ]
    },
    "claims": {
      "given_name": "Max",
      "family_name": "Mustermann",
      "birthdate": "1956-01-28",
      "place_of_birth": {
        "country": "DE",
        "locality": "Musterstadt"
      }
    }
  }
}
```

Fragen & Antworten