Christoph Döpmann

SE Electronic Identity
Humboldt-Universität zu Berlin
Wintersemester 2012/2013

OpenID

Gliederung

- Überblick
- Funktionsweise im Detail
- Bewertung
- Ausblick

Überblick

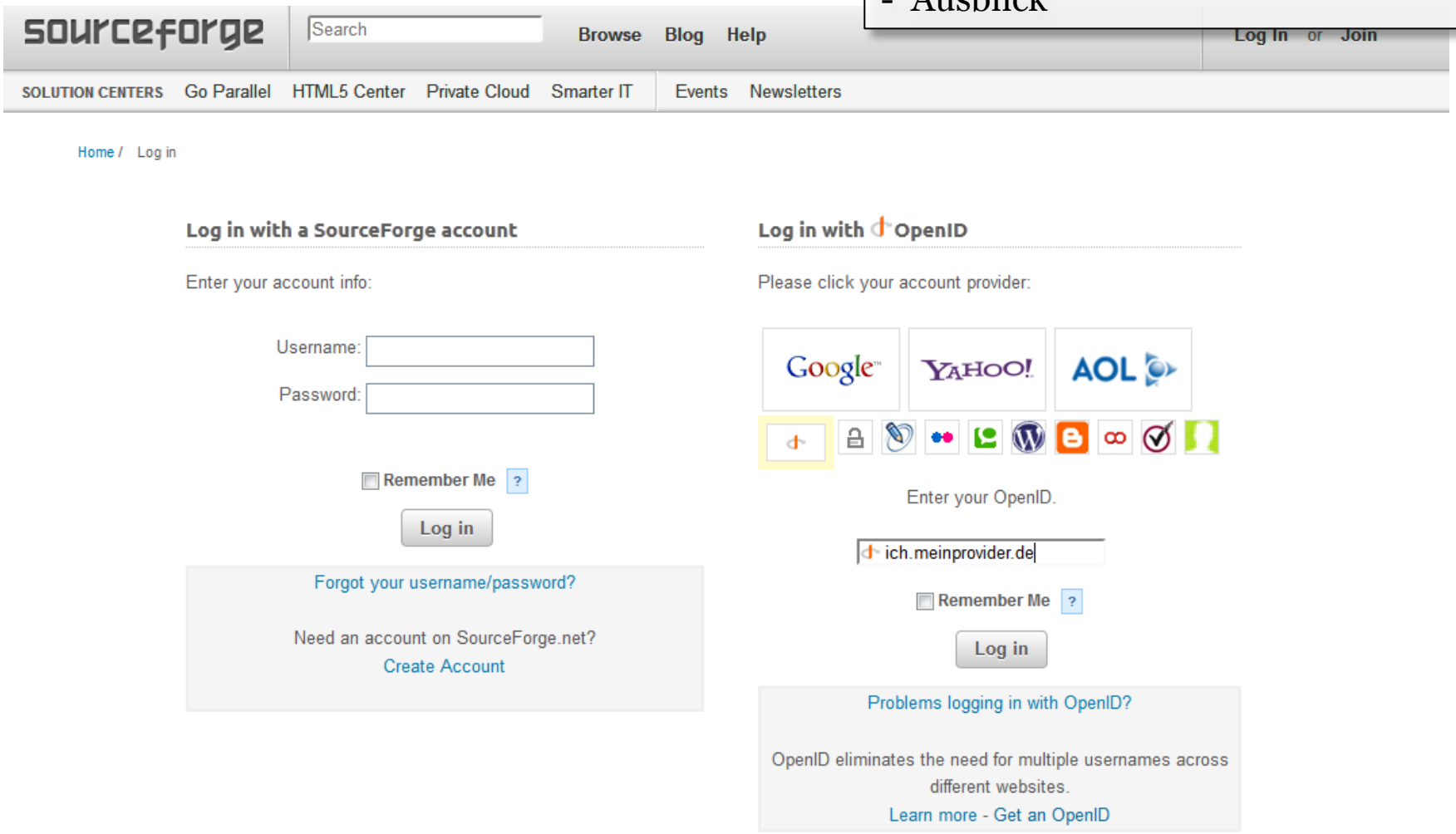
- offenes „Single-Sign-On“-Protokoll
- heute gibt es die OpenID Foundation
  - Microsoft
  - Google
  - Yahoo
  - Facebook
  - …
- seit 2007: OpenID 2.0

- Überblick
- Funktionsweise im Detail
- Bewertung
- Ausblick

Motivation

- Problem: zu viele Login-Daten für zu viele Web-Services
- OpenID‘s Lösung: eine Identität für alle Dienste
  - dezentral organisiert
  - Identität = URI eines OpenID-Providers

- Überblick
- Funktionsweise im Detail
- Bewertung
- Ausblick



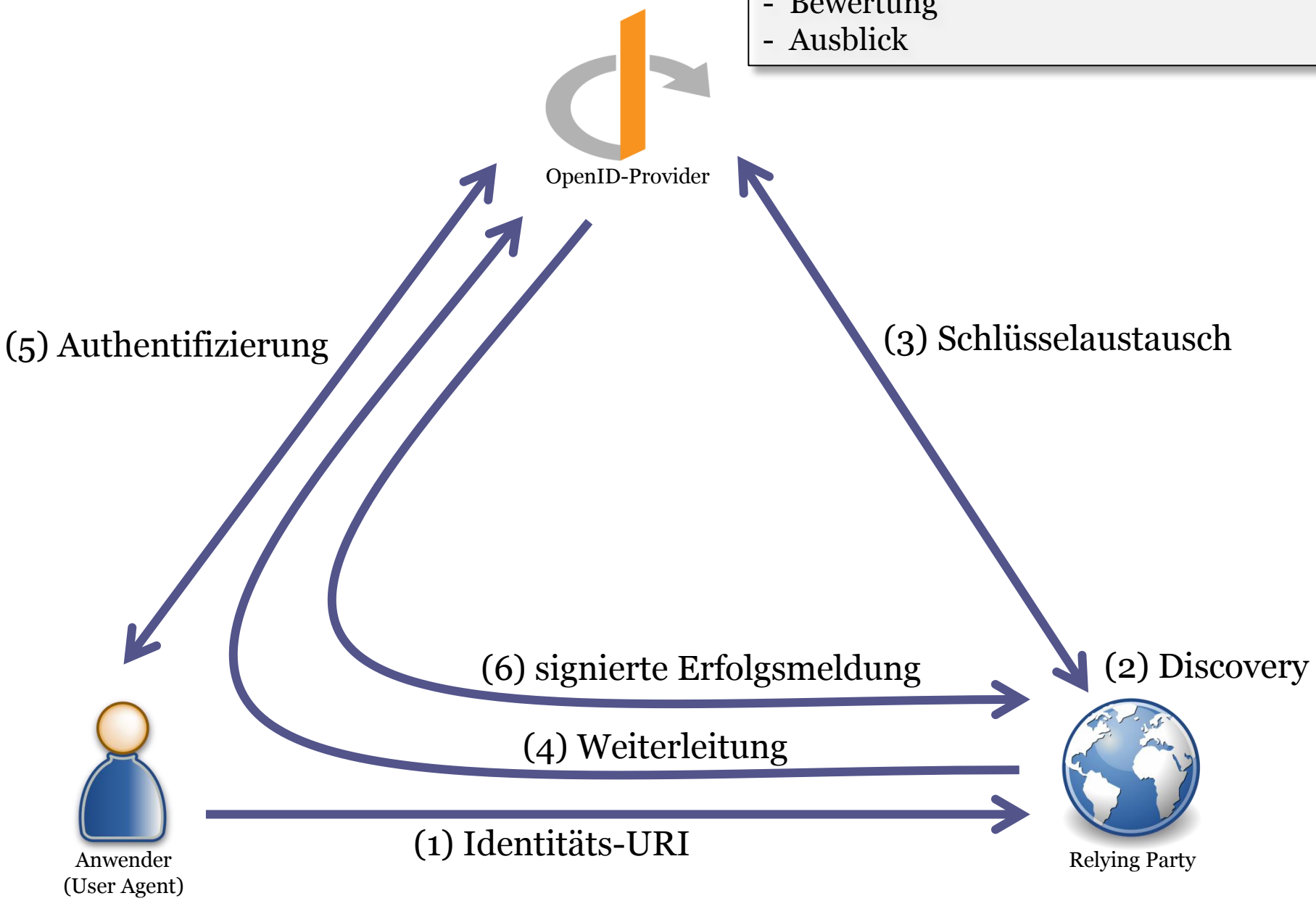
Begriffe

- OpenID-Provider (OP)
  - Dienst, der die Identität des Benutzers verwaltet
- Relying Party (RP)
  - Dienst, bei dem man sich mittels OpenID anmelden möchte
- Identität
  - URI, die dem Benutzernamen entspricht (z.B. ich.meinprovider.de)

Funktionsweise im Detail

- Anwender muss Account/Identität bei einem Provider haben
- Anwender gibt RP seine Identität (URI) an
- RP ermittelt daraus Login-Adresse des OP (Discovery) und leitet Anwender dorthin weiter
- OP authentifiziert Benutzer und leitet ihn mit signierter Erfolgsmeldung an RP weiter

- Überblick
- Funktionsweise im Detail
- Bewertung
- Ausblick



Discovery

- Zentraler Aspekt des Protokolls (auch der Sicherheit)
- Übersetzt Identität in nutzbare Server-Adresse des OP, z.B.:
  - ich.meinprovider.de → https://www.meinprovider.de/endpoint
- ID wird als Adresse interpretiert
- HTML-Tag oder HTTP-Header enthalten Verweis auf den Provider-Endpoint
- ermöglicht Delegation

- Überblick
- Funktionsweise im Detail
- Bewertung
- Ausblick

Request-Parameter

- openid.mode

  Value: "checkid_immediate" or "checkid_setup"

  Note: If the Relying Party wishes the end user to be able to interact with the OP, "checkid_setup" should be used. An example of a situation where interaction between the end user and the OP is not desired is when the authentication request is happening asynchronously in JavaScript.

- openid.claimed_id

  Value: (optional) The Claimed Identifier.

  "openid.claimed_id" and "openid.identity" SHALL be either both present or both absent. If neither value is present, the assertion is not about an identifier, and will contain other information in its payload, using **extensions**.

  It is RECOMMENDED that OPs accept XRI identifiers with or without the "xri://" prefix, as specified in the **Normalization** section.

- openid.identity

  Value: (optional) The OP-Local Identifier.

  If a different OP-Local Identifier is not specified, the claimed identifier MUST be used as the value for openid.identity.

  Note: If this is set to the special value "http://specs.openid.net/auth/2.0/identifier_select" then the OP SHOULD choose an Identifier that belongs to the end user. This parameter MAY be omitted if the request is not about an identifier (for instance if an extension is in use that makes the request meaningful without it; see openid.claimed_id above).

- openid.assoc_handle

  Value: (optional) A handle for an association between the Relying Party and the OP that SHOULD be used to sign the response.

  Note: If no association handle is sent, the transaction will take place in **Stateless Mode**.

- openid.return_to

  Value: (optional) URL to which the OP SHOULD return the User-Agent with the response indicating the status of the request.

  Note: If this value is not sent in the request it signifies that the Relying Party does not wish for the end user to be returned.

  Note: The return_to URL MAY be used as a mechanism for the Relying Party to attach context about the authentication request to the authentication response. This document does not define a mechanism by which the RP can ensure that query parameters are not modified by outside parties; such a mechanism can be defined by the RP itself.

- openid.realm

  Value: (optional) URL pattern the OP SHOULD ask the end user to trust. See **Section 9.2**. This value MUST be sent if openid.return_to is omitted.

  Default: return_to URL

Erweiterungen

- Von Hause aus keine Übermittlung von Benutzer-Attributen u.ä.
- OpenID 2.0 sehr gut erweiterbar, häufig verwendete Extensions:
  - Simple Registration
  - Attribute Exchange

Bewertung

- als Ersatz für Passwort-Manager zu sehen
- problematisch in Hinsicht auf Privatsphäre und Sicherheit
- Entwurf und Umsetzung der Spezifikation beeinflusst von kommerziellen Absichten der Förderer

Probleme mit der Privatsphäre

- größtes Manko von OpenID: Der Provider kann alle Anmeldungen des Benutzers verfolgen
- gerade große OpenID-Provider haben Interesse an Profilbildung
- Lösung: Eigener OpenID-Provider?
  - \+ viele freie Implementationen
  - – Spezifikation lässt den RP Raum zum Einschränken der Provider (2.0)
  - – nur für wenige praxisrelevant
  - – Profilbildung durch RP möglich

- Überblick
- Funktionsweise im Detail
- Bewertung
- Ausblick

Sicherheitsprobleme

- anfällig gegen Phishing
  - bösartige RP könnte auf MITM-Seite weiterleiten
- Sicherheit der Auflösung Identität -> Provider beruht auf Sicherheit von DNS
  - DNS-Spoofing ist realistisch
- alle Accounts nur so sicher wie der des Providers

- Überblick
- Funktionsweise im Detail
- Bewertung
- Ausblick

Akzeptanzproblem

- „Alle Anbieter wollen nur Provider sein.“
  - erhöht die eigene Präsenz und Reichweite
- Als Relying Party gibt man Macht aus der Hand
  - hauptsächlich interessant für kleine Seiten

Fazit

- geringe Komfort-Verbesserung gegenüber Passwort-Manager wiegt Nachteile nicht auf
- nicht so dezentral wie gewünscht
- große Provider profitieren am meisten

Ausblick

- OpenID gewinnt immer mehr an Verbreitung
  - Massenfähigkeit ist allerdings umstritten
- alternativer Ansatz: OpenID Connect
  - Verbindung von OpenID mit OAuth
  - Anmeldebestätigung selbst ist OAuth-Scope

Quellen (abgerufen am 12.11.2012)

- http://openid.net/specs/openid-authentication-2_0.html
- http://www.theserverside.com/news/1364125/Using-OpenID
- http://en.wikipedia.org/wiki/OpenID
- http://www.untrusted.ca/cache/openid.html
- http://www.heise.de/security/meldung/Online-Authentifizierungsmechanismus-OpenID-in-Version-2-0-168123.html
- http://nat.sakimura.org/2012/01/20/openid-connect-nutshell/
- http://lists.openid.net/pipermail/openid-general/2007-May/002386.html
- http://openid.net/specs/openid-connect-basic-1_0-15.html
- http://www.heise.de/developer/artikel/Step2-Protokoll-OpenID-und-OAuth-Hand-in-Hand-1359904.html