Usable Security

Usable Security

- If a security procedure is too difficult, users
  - may configure it incorrectly,
  - may use it incorrectly,
  - won't deploy it, or
  - will just switch it off.
- Security vs. „ease of use“

If it is not **usably secure**,
it's not
the **Internet of Things**

[Payne, Edwards 2008]

Usable Security: eine Checkliste

- Wird der **Path of least resistance** unterstützt?
- **Active authorization** (aktive Zustimmung erforderlich)
- **Revocability**
- **Visibility** (of the authority of others)
- **Self-awareness** (of the user's own authority)
- **Expressiveness** … in terms that fit the user's task.
- **Relevant boundaries, Identifiability**
- **"Foresight"** (support a working mental model)
- **Trusted path**

Bild mit freundlicher Genehmigung von The Natural Navigator
https://www.naturalnavigator.com/contact/

[Payne, Edwards 2008]

Usable Security: eine Checkliste

- Wird der **Path of least resistance** unterstützt?
- **Active authorization** (aktive Zustimmung erforderlich)
- **Revocability**
- **Visibility** (of the authority of others)
- **Self-awareness** (of the user's own authority)
- **Expressiveness** … in terms that fit the user's task.
- **Relevant boundaries, Identifiability**
- **"Foresight"** (support a working mental model)
- **Trusted path**

PEBKAC: Phishing

- Nutzer dazu verleiten, vertrauliche Information in eine (gefälschte) Webseite zu tippen
- Problem: TLS überprüft nur Übereinstimmung Domainname/Zertifikat
  - Nutzer muß Domainnamen selber prüfen ➜ `paypa1.com`
- „Antwort“: Extended validation (EV)-Zertifikate
  - Adreßzeile grün, Angabe Organisationsname (Firefox/Safari)
- Erkennung von irreführenden Links, Blacklists, ... (rot!)

Vertrauen: Mentales Modell

- Wir sind gewohnt, nach dem Aussehen zu urteilen
  - genauer: nach Kompetenzsignalen
- Digitales Aussehen läßt sich zu leicht fälschen

- Konsequenzen des Handelns schwer abzusehen
  - Habituelles „Wegclicken“
  - Wer versteht Zertifikate?

Problem: zu viele Passwörter

- Überall das gleiche Passwort?
- Hunderte von Passwörtern merken?
  - ...und immer wieder eintippen (habituell!)
  - 1password etc...
- SSO: Single sign-on
  - Trennung Identity Provider (IdP) vs. Relying Party (RP)
  - Einmalige Authentisierung bei IdP
  - Verschiedene RP können diese Authentisierung nutzen
    - Service Provider (SP)

Was ist eine Identität

- Bedeutungsloser Name (cabo@tzi.org)
- Attribute:
  - E-Mail-Adresse (cabo@tzi.org)
  - Name: Carsten Bormann
  - Adresse, Geburtsdatum, Familienstand, Abiturnote...
  - Sexuelle Präferenz, Vorstrafen, Gesundheitsstatus, ...
- Attribute Release Policy

Trends des Identitätsmanagements

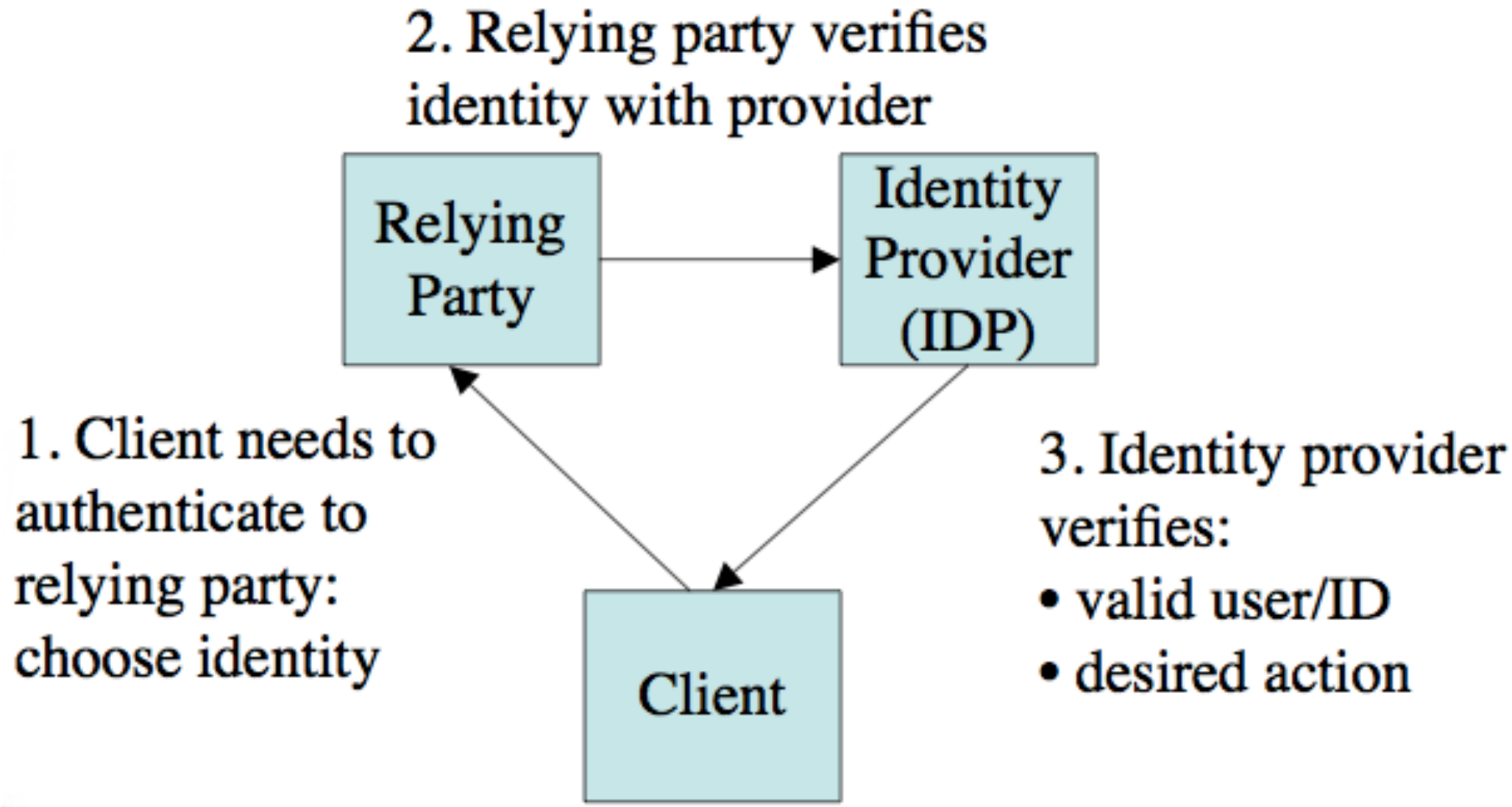
Ansätze

- Unternehmenszentriertes Identitätsmanagement
- Unternehmens-/organisationsübergreifendes Identitätsmanagement
- Benutzerzentriertes Identitätsmanagement

Unternehmenszentriertes Identitätsmanagement

Definition/Eigenschaften

- Unternehmenszentriertes Identitätsmanagement – Enterprise-Centric Identity Management
- IDM-System zur Ermöglichung von Geschäftsprozessen *innerhalb eines* Unternehmens
- Monopolistisch: Alle Komponenten des IDM-Systems wie z.B. Identity Provider (IdP) und Relying Parties (RP) sind unter der Kontrolle des Unternehmens



Quelle: Lisa Dusseault

Herausforderungen (1)

- Ermöglichung von Single-Sign On (SSO):
  - Nur ein Anmeldevorgang der Mitarbeiter, um auf alle für die Arbeit relevanten Applikationen wie z.B. SAP-Module zuzugreifen
- Unternehmensbezogenes IDM nicht nur ein technisches System, sondern auch **organisatorische Maßnahmen** erforderlich:
  - Geschäftsprozesse für das Provisioning und De-Provisioning:
    Wie werden die Anwendungen in das IDM-System eingebunden?
  - Einrichtung eines Help Desks (z.B. Zurücksetzen von Passwörtern)
  - Training der Mitarbeiter, um mit dem IDM-System umgehen zu können

Herausforderungen (2)

- Zusammenspiel zwischen IDM-System und Autorisierung:
  - Bislang: Rollen nur Attribute eines IDM-Systems
  - unternehmensweites rollenbasiertes Berechtigungsmanagement (*role-based access control*, RBAC) nötig
  - Orientierung an RBAC-Standard (ANSI-INCITS 359-2004)
  - Autorisierung vs. SSO: freie Rollenaktivierung eines Nutzers muss möglich sein
  - Umsetzung unternehmensinterner Regeln für die Autorisierung (z.B. Aufgabentrennung zwischen Rollen, Kassierer vs. Kassenprüfer)

Unternehmens-/ organisationsübergreifendes Identitätsmanagement

Motivation

- Viele unternehmensübergreifende Geschäftsprozesse
  - Geschäftsprozesse in einer Lieferkette (*supply chain*)
  - Geschäftsprozesse bei Bestellvorgängen
- Organisationsübergreifende Grids
  - Zugriff auf Daten und Rechenkapazitäten weltweit
  - Beispiele: wissenschaftliche Berechnungen (CERN), medizinische Grids
- Wie kann der Zugriff auf Ressourcen / Daten / Geschäftsprozesse organisationsübergreifend transparent und sicher geregelt werden?

Föderationen

- Bildung von Föderationen (*federations*), bestehend aus mehreren unternehmenszentrierten IDM-Systemen
  - Organisations-/unternehmensübergreifendens IDM-System
- Anschließen an Föderation
  - Aufbau einer Vertrauensbeziehung (*trust relationship*) zwischen den Mitgliedern der Föderation
- Vereinfachte Idee für externen Zugriff auf Ressourcen:
  - Bei externem Zugriff eines Benutzers handeln der lokale IdP des Benutzers und der externe SP die Attribute zur Authentisierung und Autorisierung (z.B. Benutzernamen, Rollen) transparent aus
  - Nur lokale Authentisierung des Benutzers bei eigenem IdP

Standardisierung, Protokolle für Föderationen (1)

- Security Assertions Markup Language (SAML) 2.0
  - XML-basierte Sprache
  - http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
- Zusätzliche Arbeit der Liberty Alliance
  - Mitglieder vor allem aus dem industriellen Umfeld wie z.B. Sun Microsystems, IBM, SAP, …
  - Aber auch Universitäten wie z.B. Purdue University
  - Spezifikation geeigneter Protokolle zur Authentisierung und Autorisierung; Erweiterung von SAML 2.0
  - Liberty-Föderationen
  - http://www.projectliberty.org/

Standardisierung, Protokolle für Föderationen (2)

- Shibboleth 2.0
  - Prototyp eines Rahmenwerks für ein organisationsübergreifendes IdM
  - beruht auf SAML 2.0 und den Arbeiten der Liberty Alliance
  - Entwickelt im Internet 2-Umfeld
  - Einsatz vor allem im universitären Umfeld (vor allem an US-amerikanischen Universitäten wie z.B. Penn State, Ohio State University)
  - http://shibboleth.internet2.edu

Herausforderungen und zukünftige Themen

- Festlegung geeigneter Attribute für die organisationsübergreifende Authentisierung und Autorisierung
  - Welche Rollen werden benötigt?
  - Ggf. Sicherstellung der Privacy/Anonymität der Benutzer: Nicht alle Attribute gegenüber SP veröffentlichen
- Welche konkreten Umsetzungen gibt es im industriellen Umfeld?
- Einbindung von nicht-web-basierten IT-Systemen:
  - Zum Beispiel Voice over IP

Benutzerzentriertes Identitätsmanagement

Definition/Eigenschaften

- Benutzerzentriertes Identitätsmanagement –
  User-Centric Identity Management
- Zugriff von *einzelnen Web-Benutzern* auf Web-Anwendungen verschiedener Anbieter mittels *einer ID*; „ein Benutzername für alle Web-Seiten“
- Öffnung von unternehmenszentrierten IDM-Systemen für externe Einzelbenutzer meist keine Alternative
- Mehrere konkurrierende Trusted Third Parties als IdPs;
  Monopol eines IdPs würde nicht akzeptiert werden

7 laws of identity

- 1. User Control and Consent
- 2. Minimal Disclosure for a Constrained Use
- 3. Justifiable Parties
- 4. Directed Identity
- 5. Pluralism of Operators and Technologies
- 6. Human Integration
- 7. Consistent Experience Across Contexts

Kim Cameron, 2004

1 User Control and Consent

- Technical systems must only reveal information with the user's [informed] consent.

2 Minimal Disclosure for a Constrained Use

- The solution which discloses the least amount of information and best limits its use is the most stable long term solution.

3 Justifiable Parties

- Systems must be designed so the disclosure of information is limited to parties having a necessary and justifiable place in a given relationship.

4 Directed Discovery and Authorization

- A system must support both "omni-directional" information sets for general use and "unidirectional" information sets for use within specific private authorization relationships, thus facilitating discovery while preventing unnecessary release of correlation handles.

5 Pluralism of Operators and Technologies

- A universal system must channel and enable the inter-working of multiple technologies run by multiple providers.

6 Human Integration

- The system must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against attacks.

7 Consistent Experience Across Contexts

- The system must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

Info[rmation]card: Microsofts Identity Metasystem

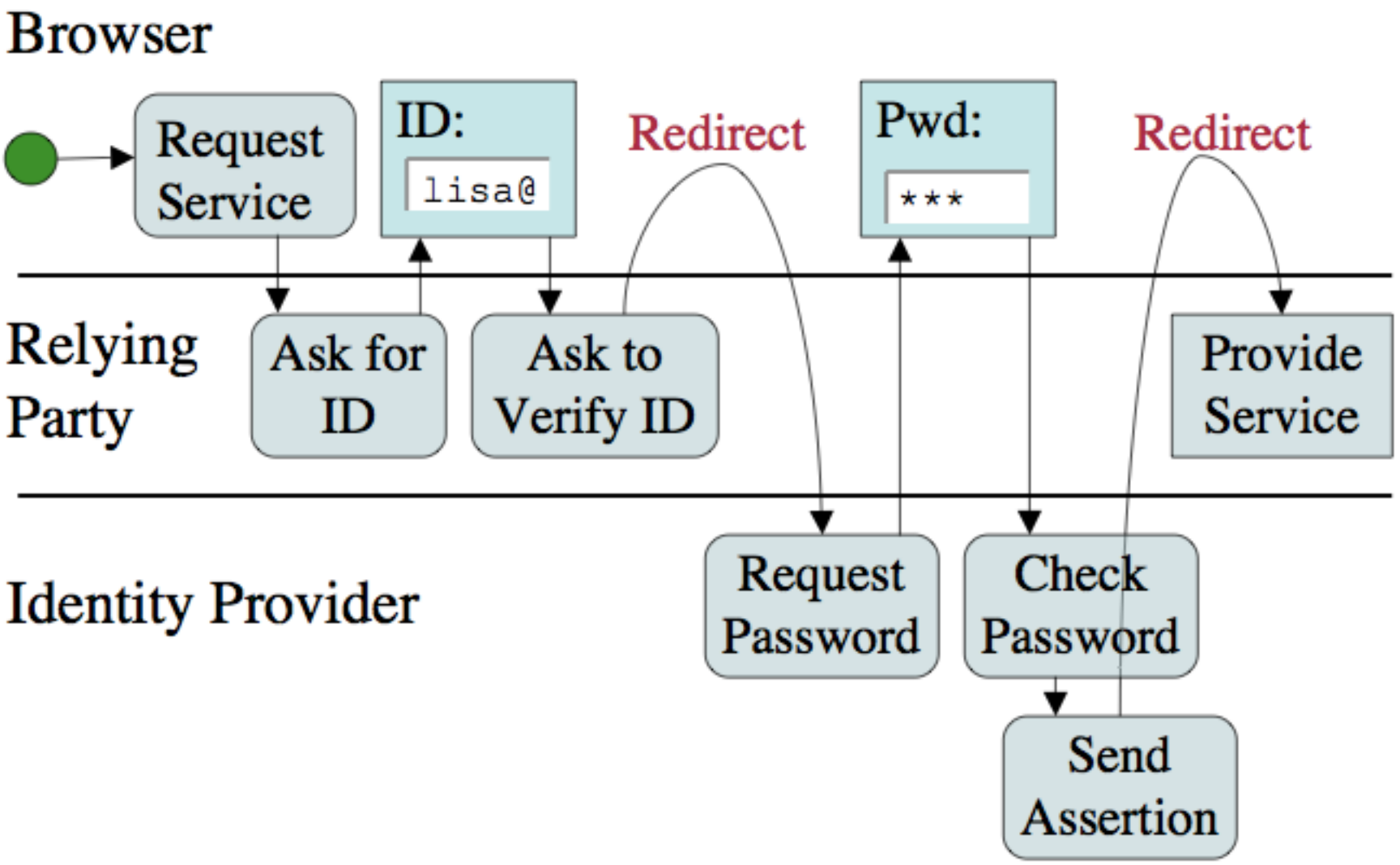
- Managed vs. Self-issued Cards
  - Wer „unterschreibt“ die *claims* (Attribute)
- Benutzt WS-*
  - Anfrage über HTML-Element <object>, Identity Selector
  - STS: Security Token Service (für managed cards)
- Windows-Implementierung: CardSpace (in .NET 3.0)
- Konsistentes UI: Karten (wie Plastikkarten!)
- Benutzer hat volle Kontrolle darüber, welche Attribute weitergegeben werden

Open-Source: Higgins

URIs für Benutzerzentriertes IDM

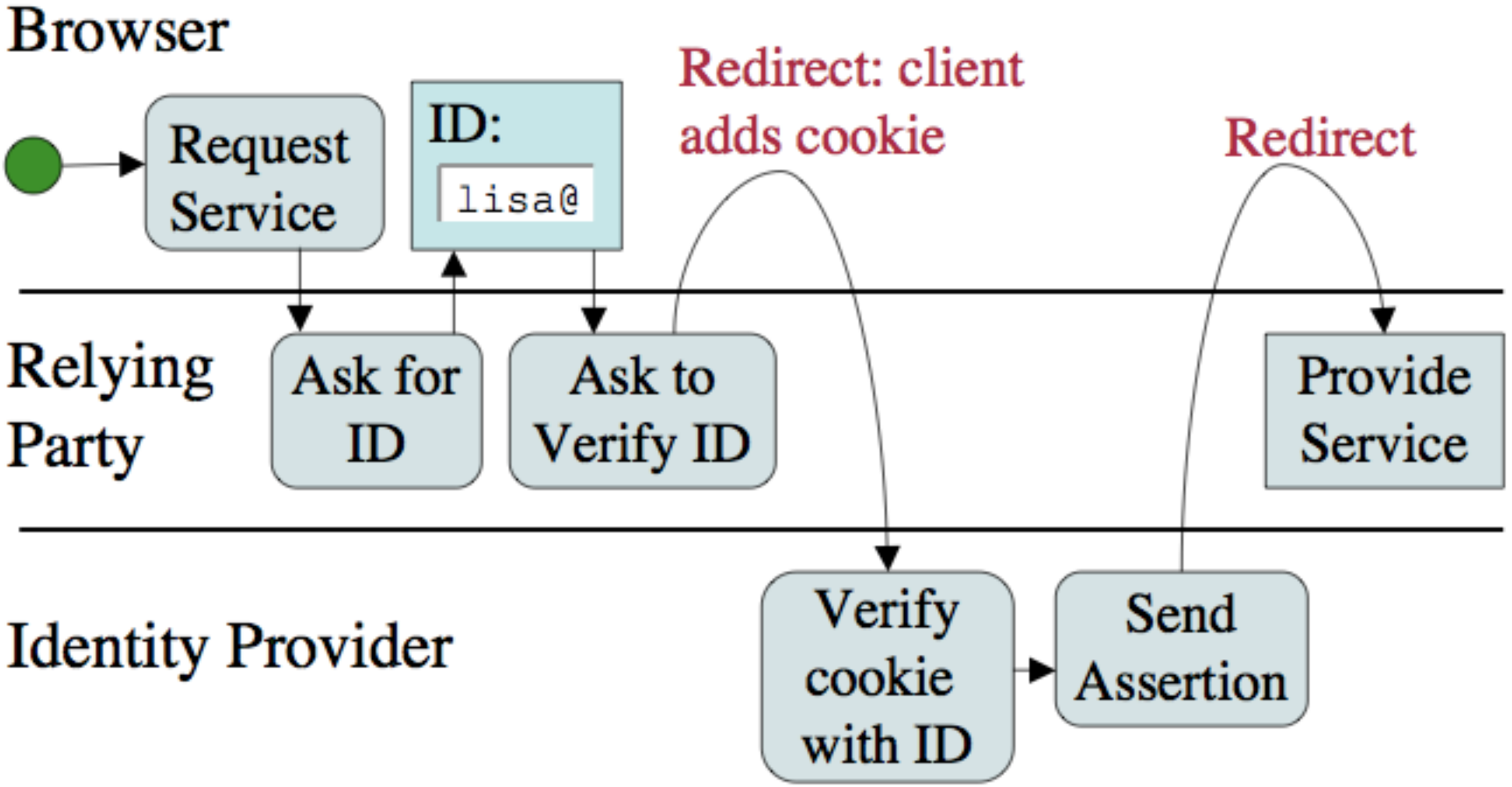
- Einige Vorschläge für das benutzerzentrierte IDM mit **URIs** unter dem Label YADIS (Yet Another Distributed Identity System):
  - Welches Protokoll, z.B. OpenID, LID (Light Weight Identity), ...
- **OpenID**-Codebibliotheken für PHP, Perl, Python, Ruby
- Idee von OpenID:
  - OpenID-URL als Benutzernamen
  - Nutzer meldet sich bei IdP mit URL und Passwort an
  - Austausch der entsprechenden Attribute und Verifikation der Identität zwischen IdP und Web-Seiten (SP) im Hintergrund

Browser-based workflow (not logged in)



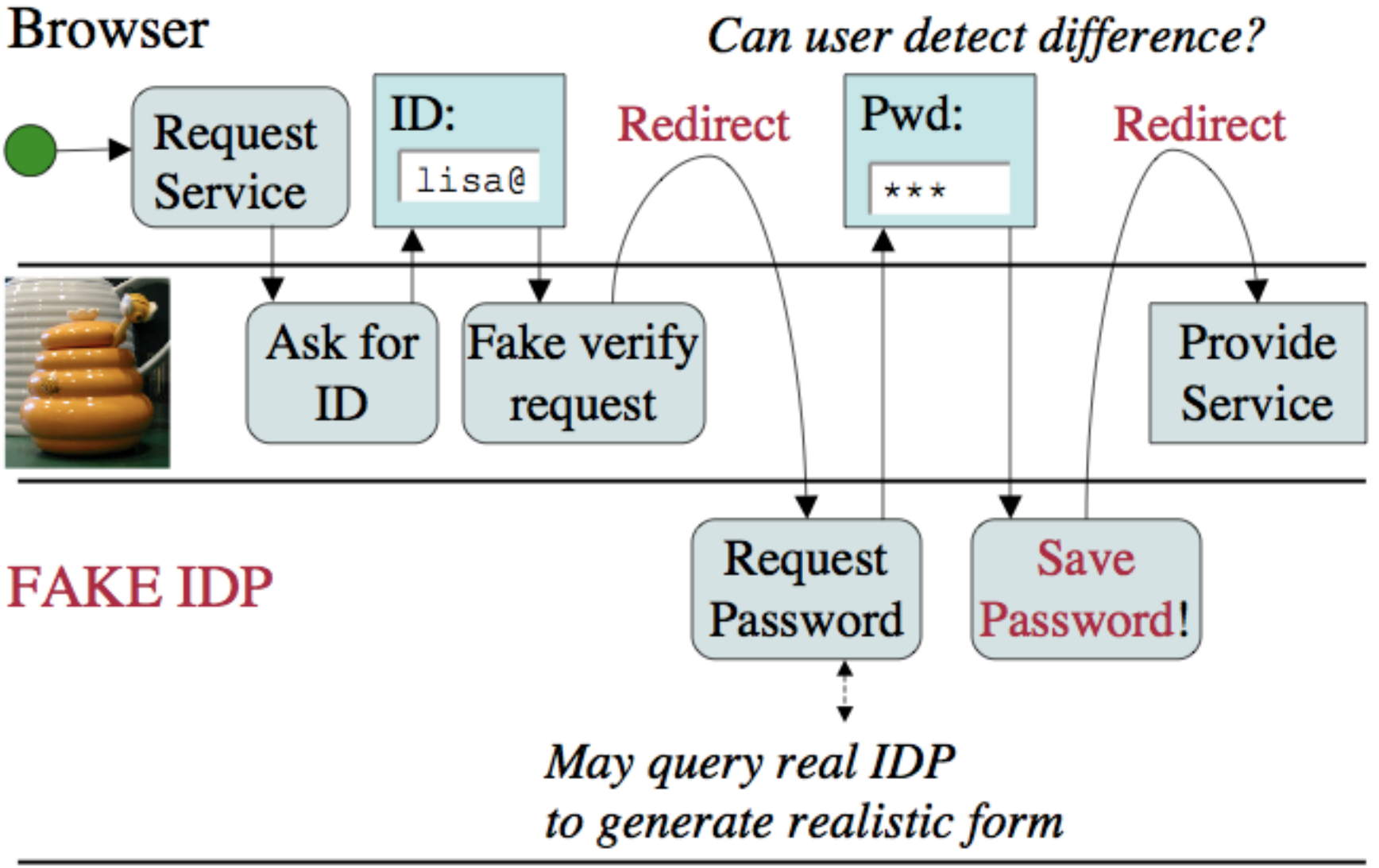
Quelle: Lisa Dusseault

Browser-based workflow (logged in)



Quelle: Lisa Dusseault

Honeypot Workflow



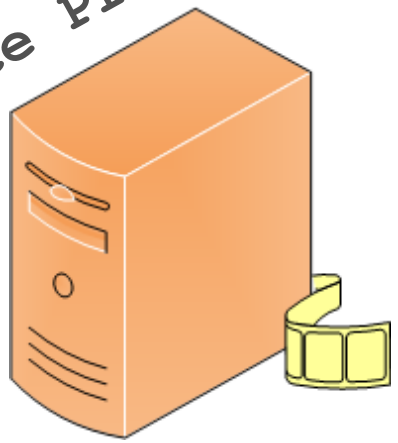
Quelle: Lisa Dusseault

OAuth: Delegation

- RP2 möchte Daten von RP1 benutzen
  - Heute: Nutzer tippt RP1-Passwort in RP2
  - Rechteeinschränkung? Rechteentzug?
  - Geht mit OpenID gar nicht
- „Secure API **Authorization**“
  - RP2 = „Consumer“
  - RP1 = „Service Provider“
  - Request Token ➜ Access Token
- „1.0“ außerhalb der IETF definiert
- OAuth 2.0: Framework fertig, Detailstandards teilweise

oauth_love_triangle

- Service Provider



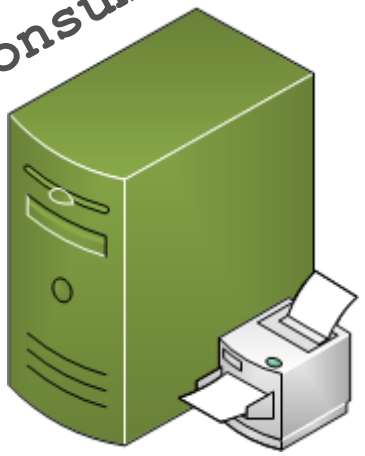
faji
foto journeys

- Protected Resources

- User

- Jane

- Consumer

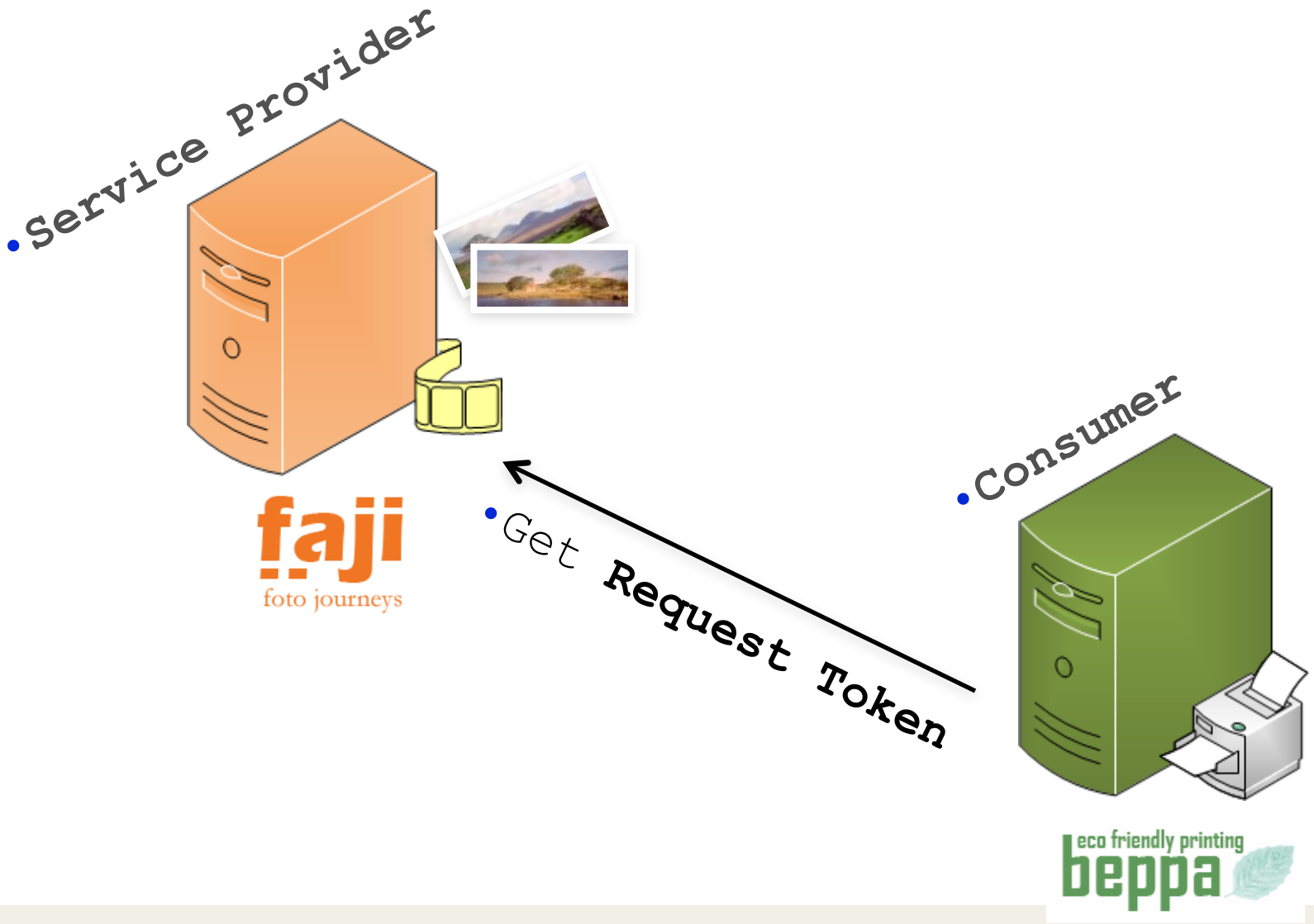


eco friendly printing
beppa

protected_resources

oauth_flow_begins

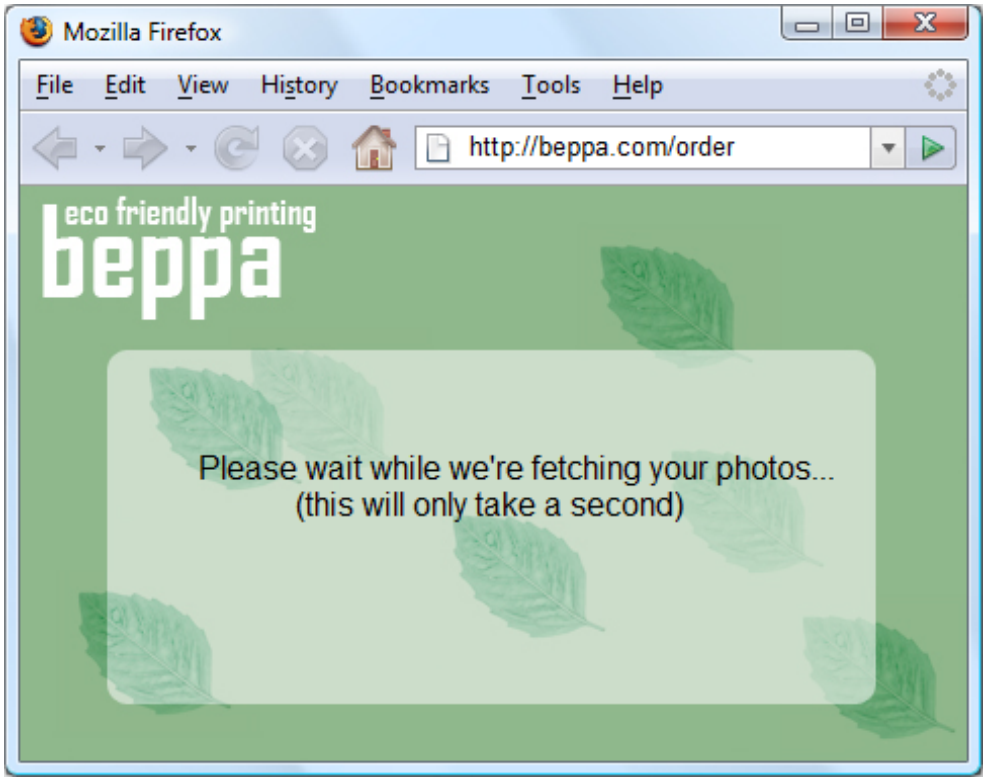
oauth_request_token



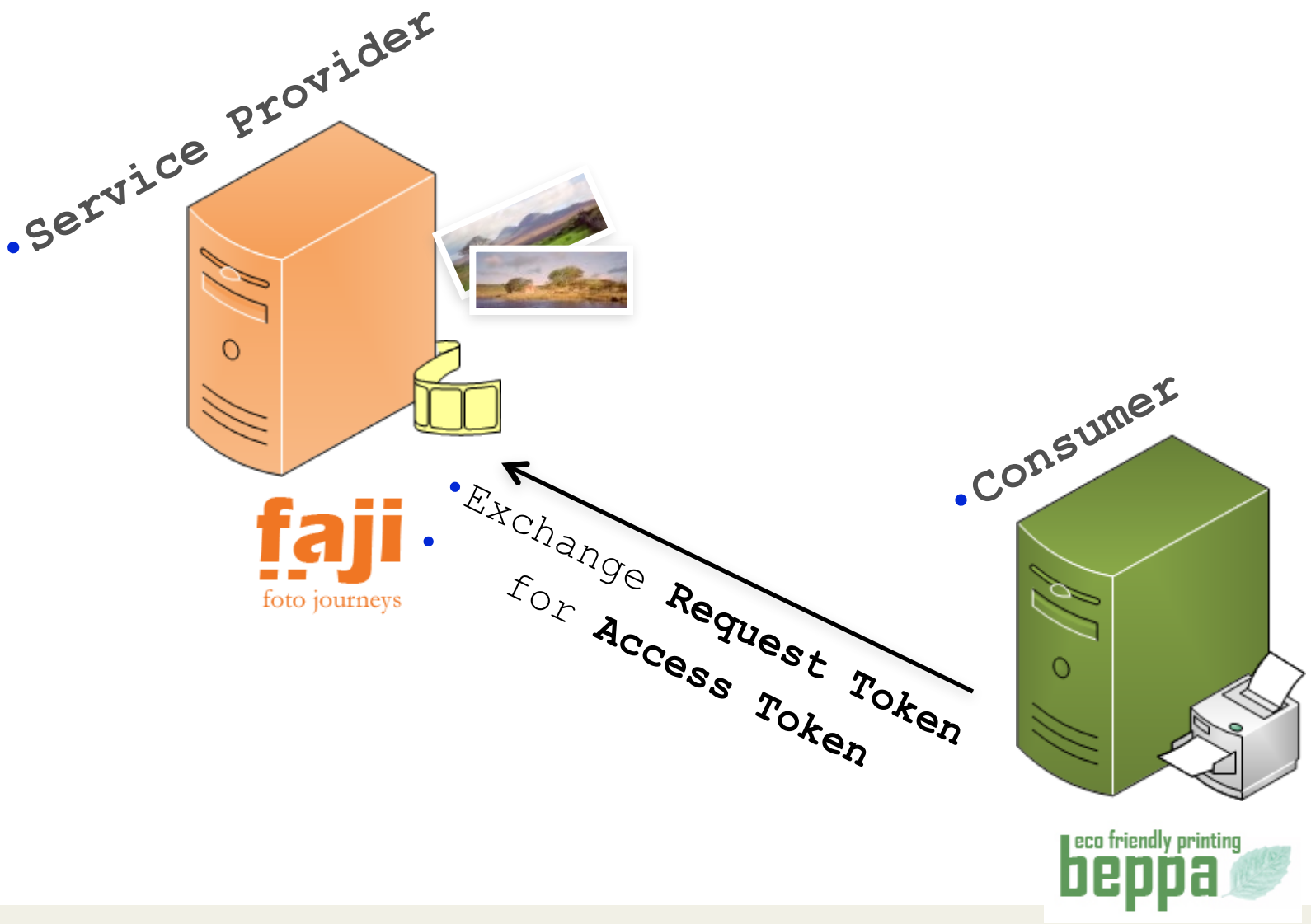
user_authentication

user_authorization

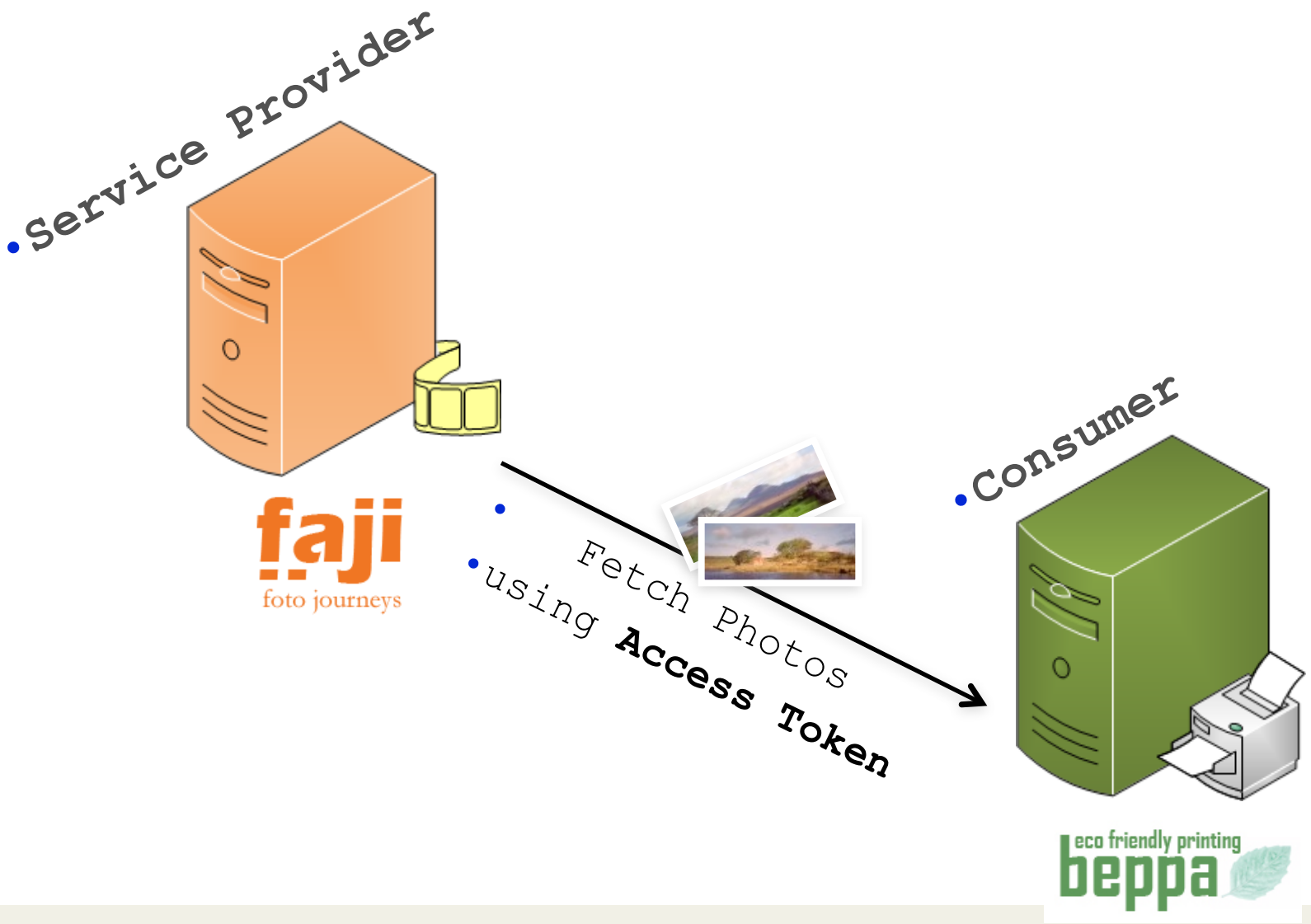
consumer_callback



oauth_access_token

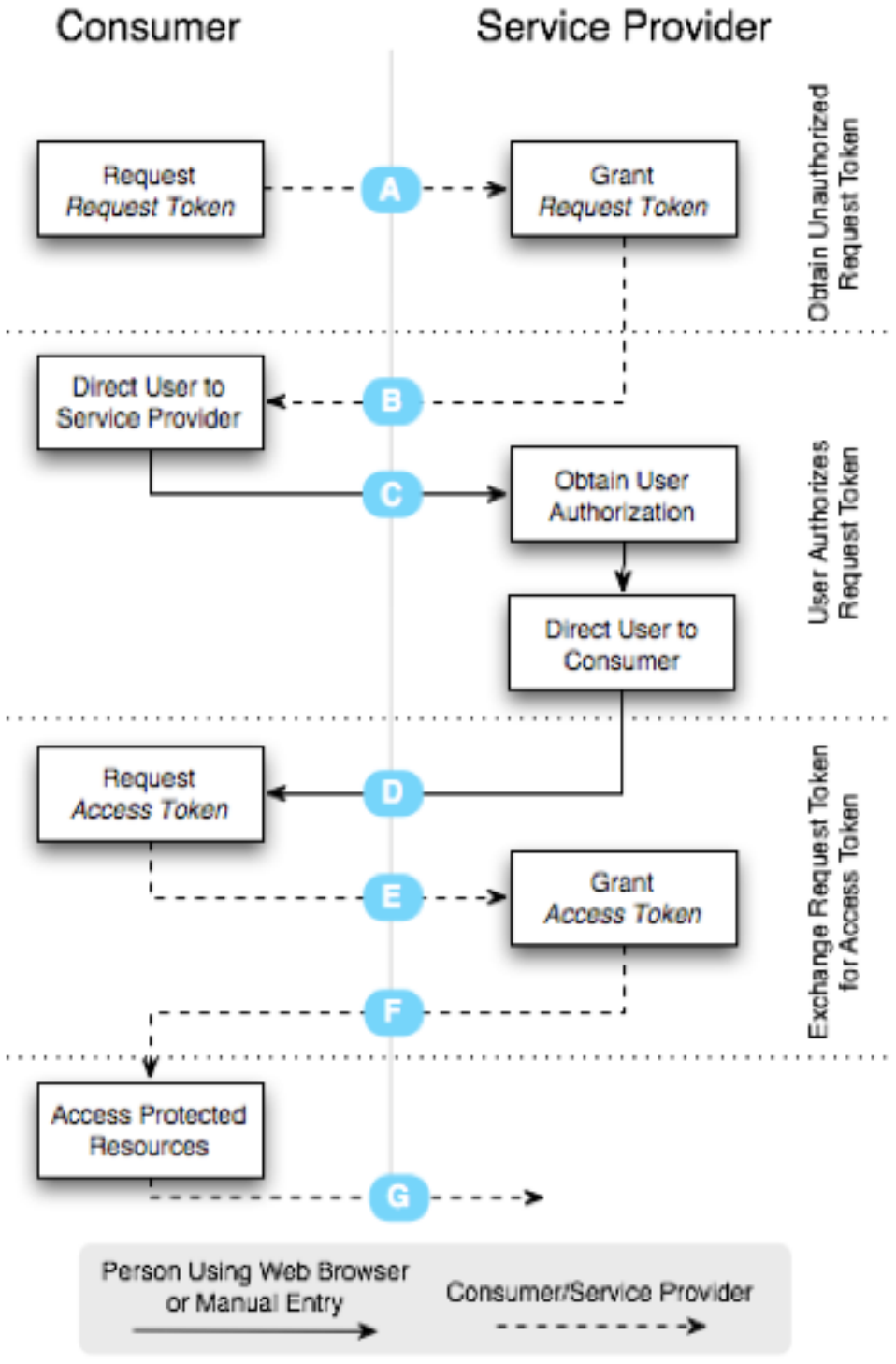


get_protected_resources



oauth_success

OAuth Authentication Flow



A Consumer Requests *Request Token*

Request includes
oauth_consumer_key,
oauth_signature_method,
oauth_signature,
oauth_timestamp,
oauth_nonce,
oauth_version (optional).

B Service Provider Grants *Request Token*

Response includes
oauth_token,
oauth_token_secret.

C Consumer Directs User to Service Provider

Request includes
oauth_token (optional),
oauth_callback (optional).

D Service Provider Directs User to Consumer

Request includes
oauth_token (optional).

E Consumer Requests *Access Token*

Request includes
oauth_consumer_key,
oauth_token,
oauth_signature_method,
oauth_signature,
oauth_timestamp,
oauth_nonce,
oauth_version (optional).

F Service Provider Grants *Access Token*

Response includes
oauth_token,
oauth_token_secret.

G Consumer Accesses Protected Resources

Request includes
oauth_consumer_key,
oauth_token,
oauth_signature_method,
oauth_signature,
oauth_timestamp,
oauth_nonce,
oauth_version (optional).

OAuth als Ersatz für OpenID, OpenID Connect

- OAuth 1.0: ein konkretes Protokoll, recht beliebt
- OAuth 2.0 (IETF): “Framework”
  - viele Varianten möglich
  - Profil nötig, um Variantenreichtum einzuschränken
- OpenID-Nachfolger **OpenID Connect**:
  Service Provider beschränkt sich auf Identitätsprüfung.
- Service Provider ➔ Identity Provider (z.B. gitlab)
  Consumer ➔ Relying Party (z.B. mattermost, hedgedoc)