isec 2024: Fragestunde

2025W04

Security is for users

Usable Security

Security braucht Usability
Usability braucht Security

Checkliste Usable Security
Beispiel Phishing
Problem: **Mentales Modell**

Identität

Namen (wie cabo@tzi.org)
Attribute (Name, …)

Datenminimierung:
Attribute Release Policy

Identitätsmanagement

1. Unternehmens-/organisationszentriert
2. Unternehmens-/organisationsübergreifend
3. **Benutzer**zentriert

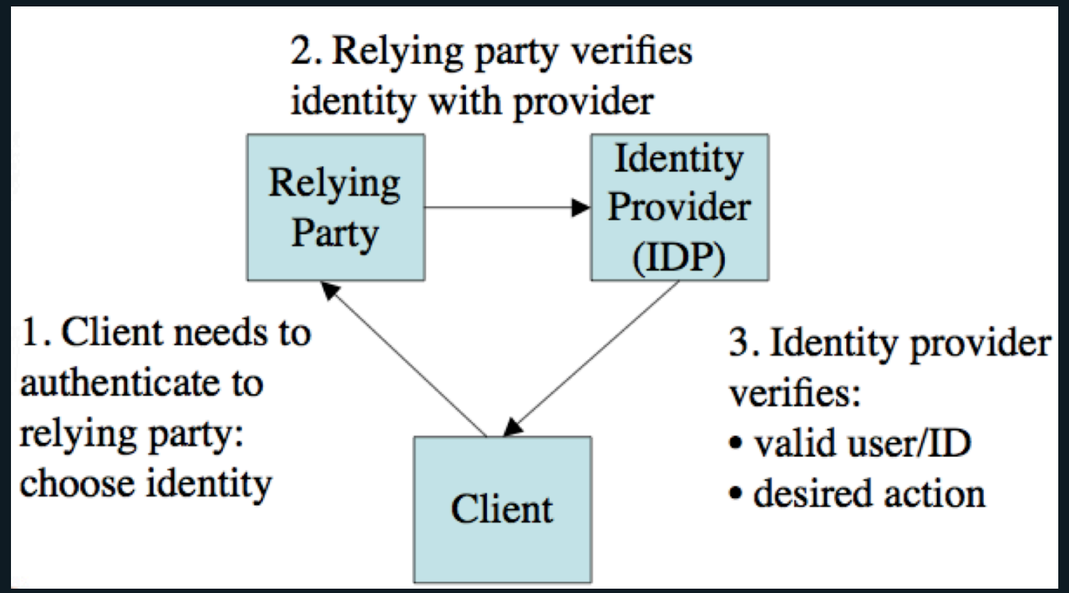
Unternehmenszentriert

Geschäftsprozesse innerhalb eines Unternehmens

Single-Sign-On (SSO)

— Organisatorische Maßnahmen

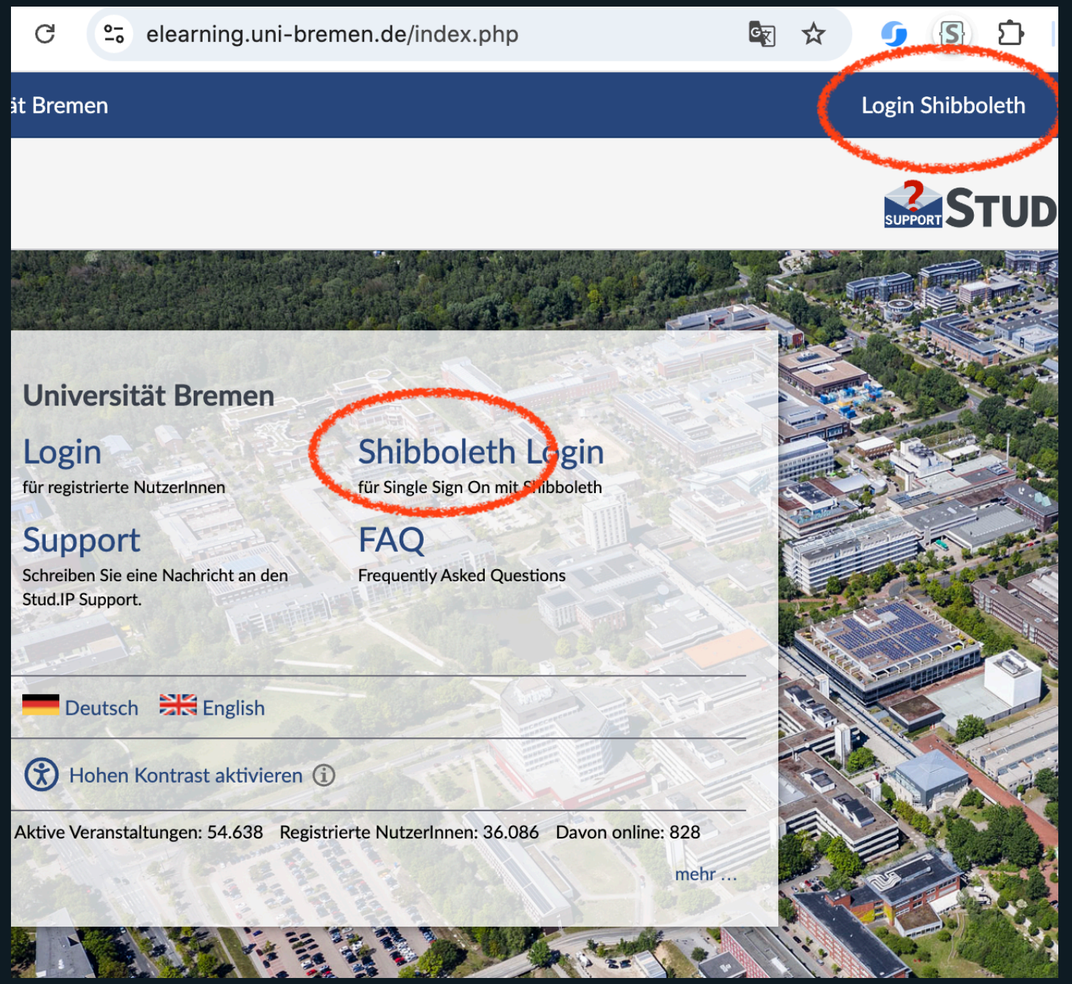
— Autorisierung?



Unternehmens-/organisationsübergreifend

Geschäftsprozesse
zwischen Unternehmen/
Organisationen

Föderationen
z.B. im edu-Bereich:
- (SAML) Shibboleth
- (RADIUS) eduroam



Benutzerzentriert

Inhaber der Identität definiert IdP dazu
- selbst betrieben?
- zentralisiert, aber: design for choice

— Facebook, Google, Apple, …

7 laws of identity

Kim Cameron, 2004

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

Systeme

OpenID: URL als Name für Identität

OAuth: Authentisierung über Autorisierung durch IdP
(OpenID Connect: Abbildung von OpenID auf OAuth)

Weiter weg von Passwörtern

OAuth verlegt Authentisierung in IdP, danach ~ SSO

WebAuthn:

— Registrierung ➔ Schlüsselpaar — bleibt auf Gerät
— Anmeldung über Nachweis des Besitzes des privaten Schlüssels

FIDO: FIDO2 mit CTAP-fähigen Geräten
vgl. Sign in with Apple