Attribut-basierte Credentials im Praxistest – mehr Datenschutz im sozialen Netzwerk einer schwedischen Schule

Harald Zwingelberg

ABC4TRUST

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Übersicht

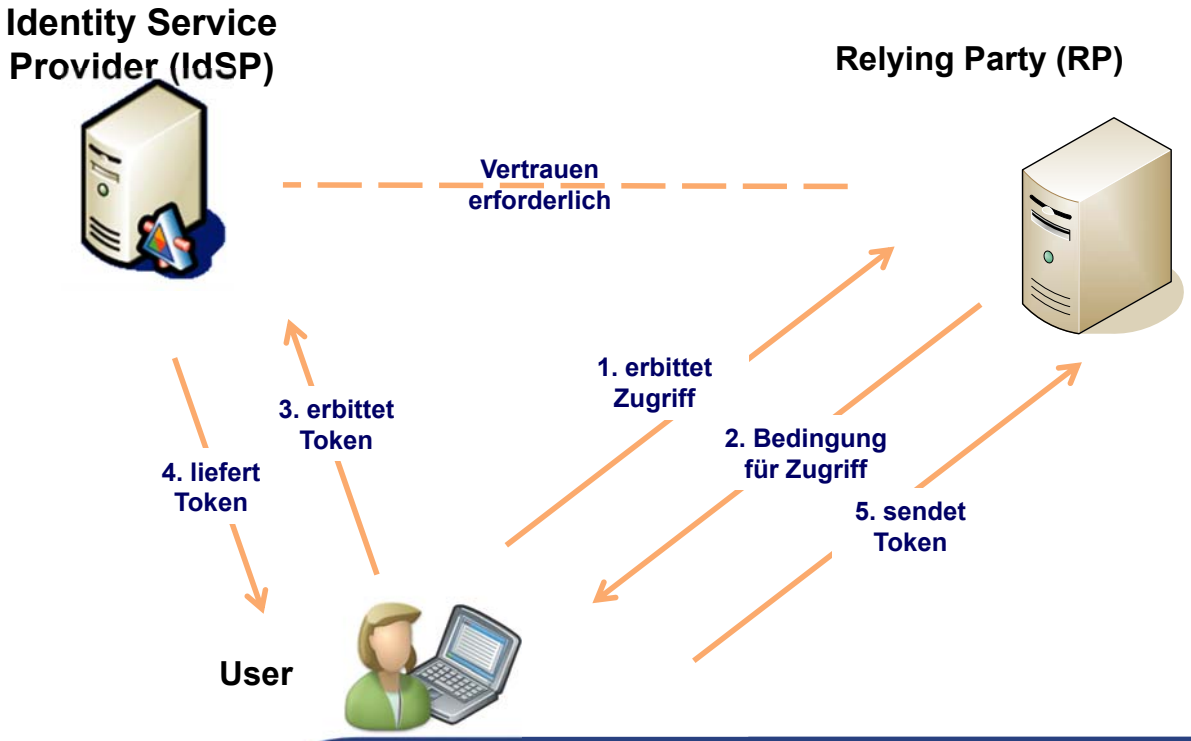
- Attribut-basierte Credentials im Überblick
- Merkmale und Möglichkeiten Attribut-basierter Credentials
- Der Anwendungstest an einer schwedischen Schule
  - Anforderungen
  - Umsetzung
  - Use cases
  - Aufdeckung von Identitäten
- Weitere Gestaltungsmöglichkeiten
- Fragen und Diskussion

Das ABC4Trust-Projekt

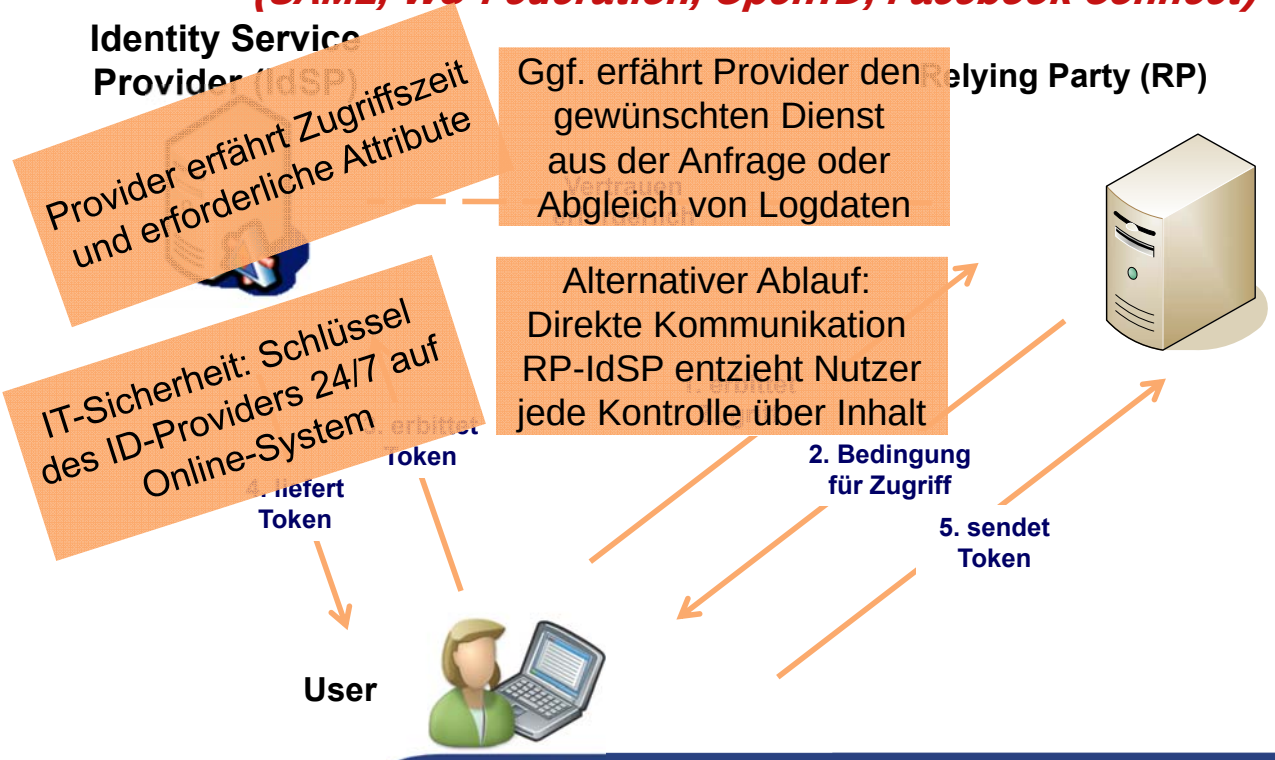
ABC4TRUST

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

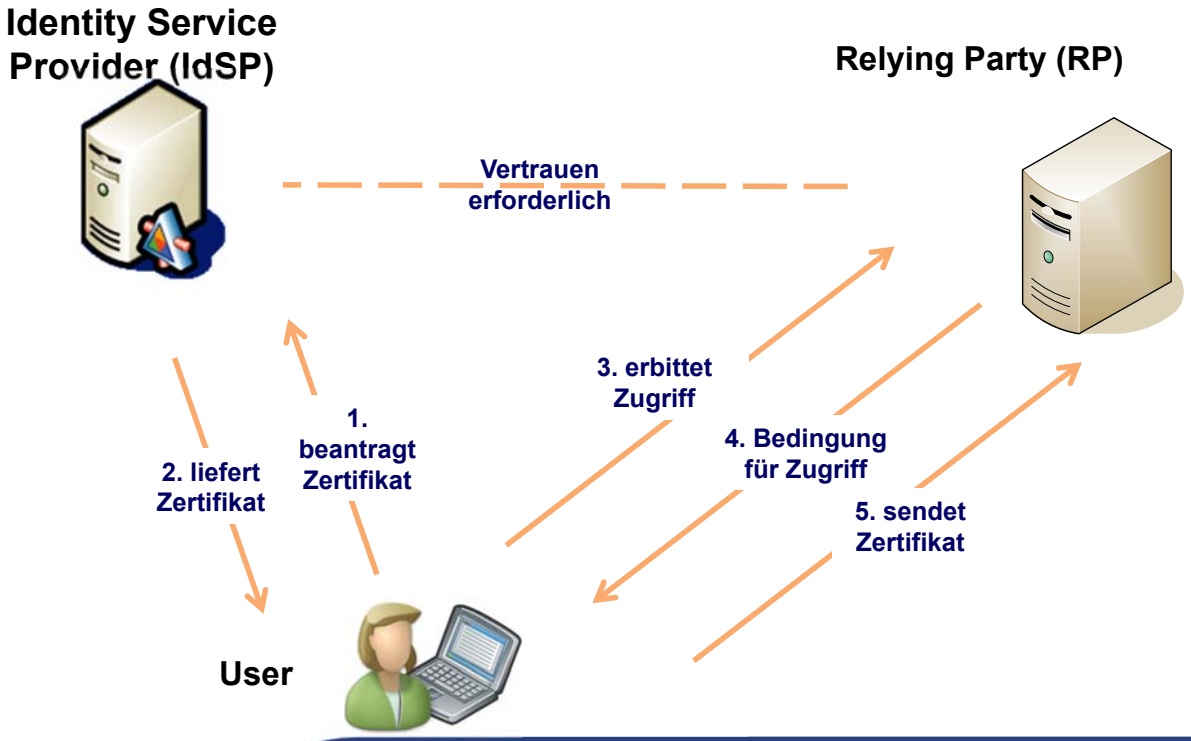
Datenschutzprobleme typischer IdM-Anwendungen (SAML, WS-Federation, OpenID, Facebook Connect)



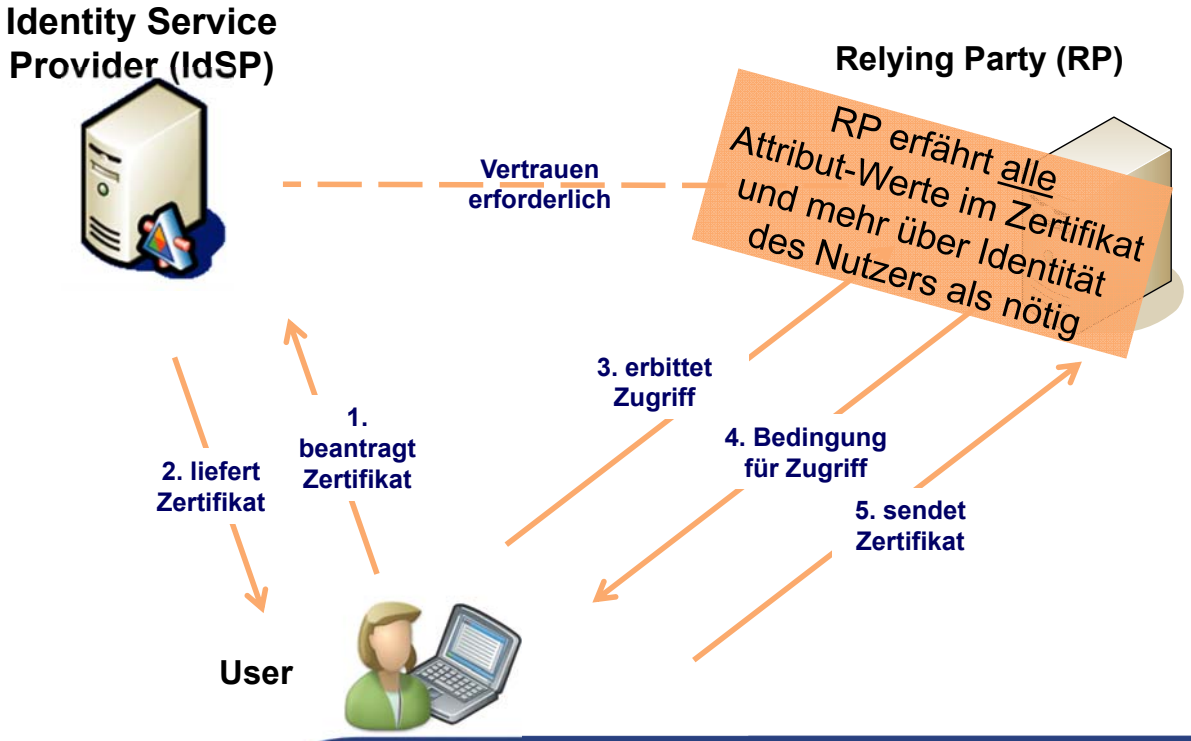
Datenschutzprobleme typischer IdM-Anwendungen (SAML, WS-Federation, OpenID, Facebook Connect)



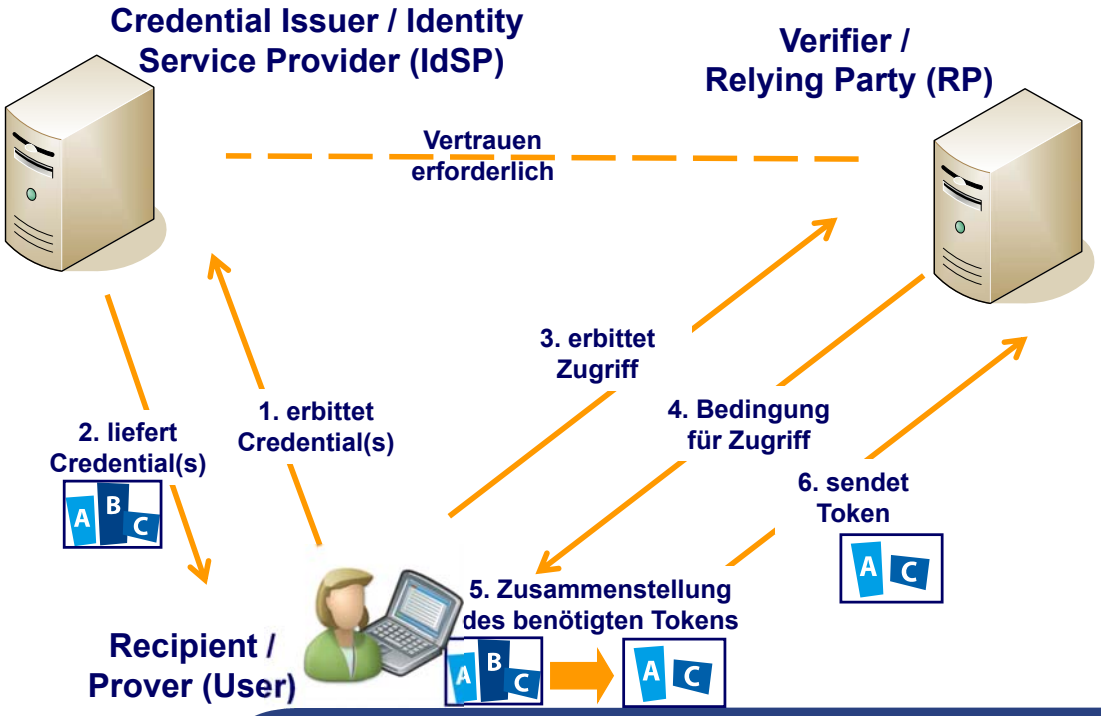
Datenschutzprobleme typischer Offline-Lösungen (X.509-Zertifikate)



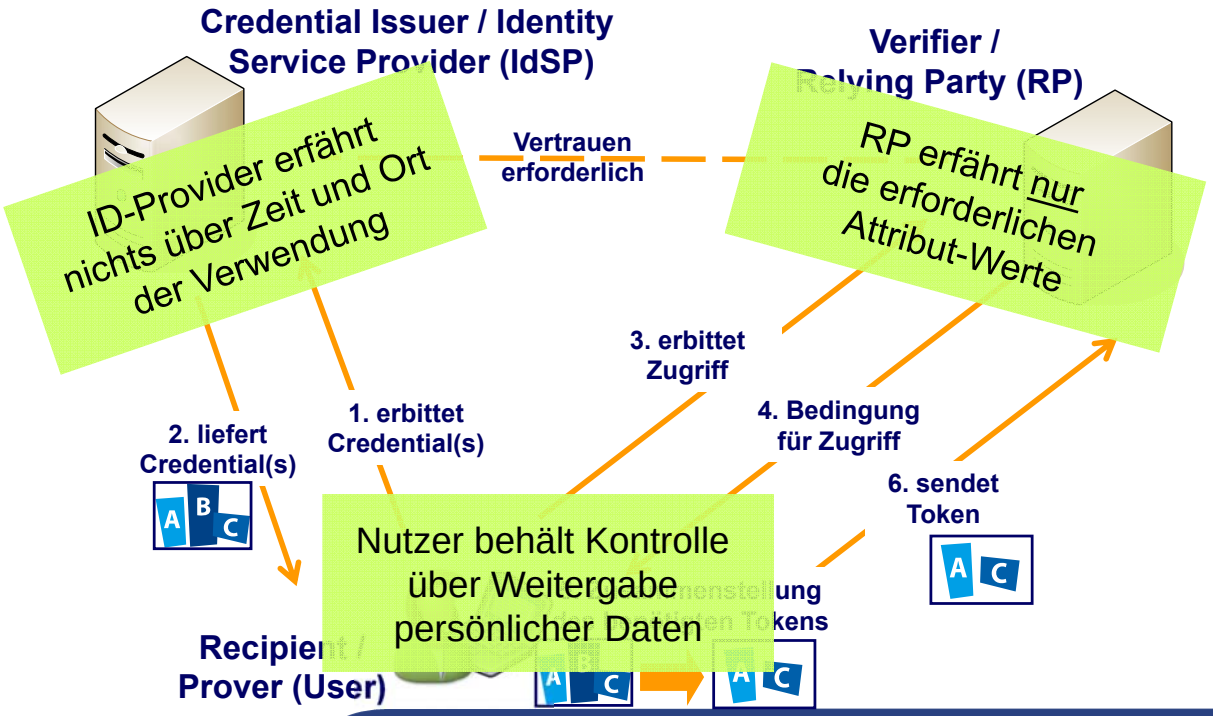
Datenschutzprobleme typischer Offline-Lösungen (X.509-Zertifikate)



Attribut-basierte Credentials (Privacy-ABCs)



Attribut-basierte Credentials (Privacy-ABCs)



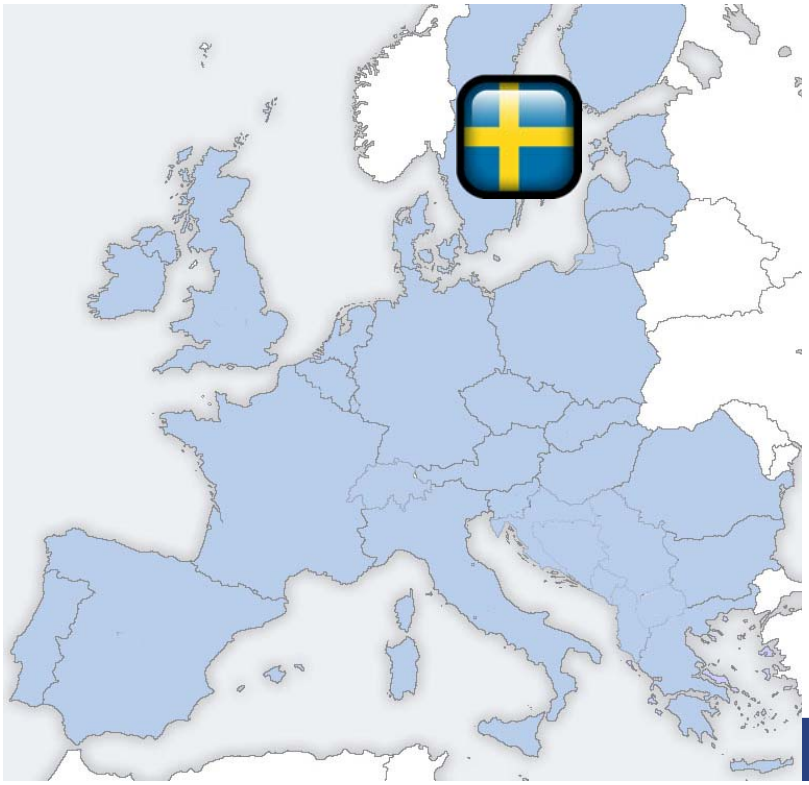
Möglichkeiten von Privacy-ABCs

- Erforderlichkeitsprinzip umsetzbar
  - Preisgabe nur von für die konkrete Verwendung erforderlichen Attributen
  - Kombination von Attributen aus unterschiedlichen Credentials mit Nachweis, dass beide zu derselben Identität gehören (Kreditkarte und Studentenausweis tragen denselben Namen, Name bleibt verdeckt)
- Nicht-Verkettbarkeit: mehrfache Verwendung lässt keine Rückschlüsse darüber zu, ob dieselbe Person handelt
- Abgeleitete Aussagen über Attribute möglich (geb. =< 27.08.1994)

Möglichkeiten von Privacy-ABCs

- Nicht-verkettbare Pseudonyme verfügbar
- Beschränkungen der Nicht-Verkettbarkeit möglich: z.B. nur 3 erlaubte Verwendungen nicht verkettbar; bei 4. Verwendung können alle verkettet werden (Umfragen, Abstimmungen)
- Widerruf von Zertifikaten (Revocation) ohne einheitliche Zertifikatsnummer, die Verkettung erlauben würde
- Spätere Aufdeckung von Identitäten (Inspection), sofern ausnahmsweise im Vorfeld bei Authentifizierung vorgesehen

Erprobung in Schweden: soziales Netzwerk



- Schulinternes soziales Netzwerk zur Kommunikation zwischen Schülern, Eltern, Lehrkörper
- Sichere und vertrauenswürdige Authentifizierung bei gleichzeitigem Schutz der Privatsphäre
- Usability: Datenschutztechnologie auch für Schüler / Jugendliche verständlich gestalten

Rahmenbedingungen

- Das Internet wird in schwedischen Schulen umfangreich genutzt:
  - Zu Recherche- und Lehrzwecken
  - Zur Kommunikation mit Schülern und Eltern

- Schwedische Schulen sind gesetzlich verpflichtet, die Eltern über Abwesenheiten zu unterrichten, individuelle Lehrpläne zu vereinbaren und die Eltern über Fortschritte zu unterrichten

- Die Authentifizierung erfolgt derzeit mittels Name und Passwort; eine sicherere, aber einfache Methode ist erwünscht

Anforderungen

- Anonyme bzw. pseudonyme Nutzung ermöglichen
- Nutzer sollen in Gruppen diskutieren können
- Kommunikation von
  - Schulpersonal - Schüler
  - Definierte Gruppen (Klassenverband, nach Alter oder Geschlecht getrennt, ...)
  - Schulpersonal - Eltern
  - einer bestimmten Person (Lehrer, Schüler, Elternteil)

  $\Rightarrow$ Authentifizierung muss Angaben verifizieren können
- Nutzbarkeit: Schüler und Eltern sollen mit dem System umgehen können

Umsetzung

- Die Teilnehmenden erhalten
  - eine Smart Card vorkonfiguriert mit Credentials und
  - Lesegeräte
- Benötigte Software wird gegenwärtig entwickelt (geplant: Plug-in für Firefox)

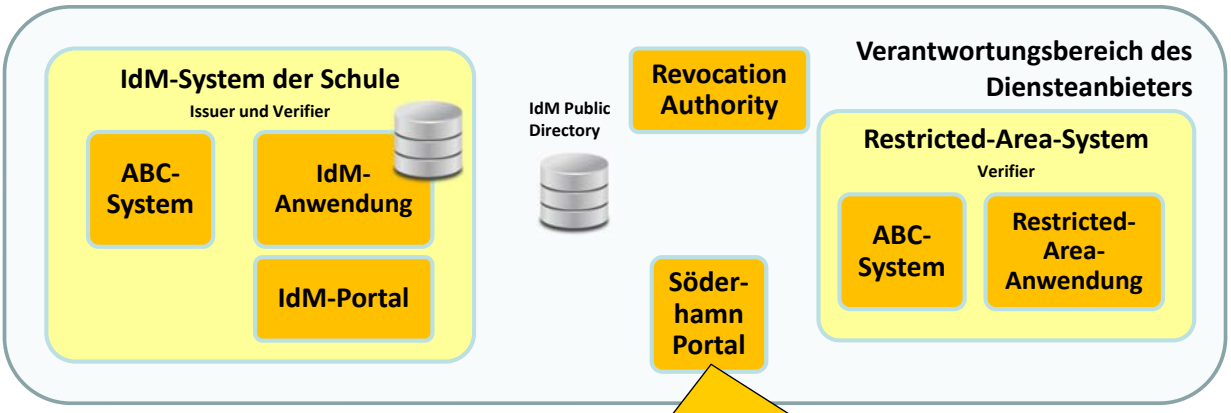
Umsetzung

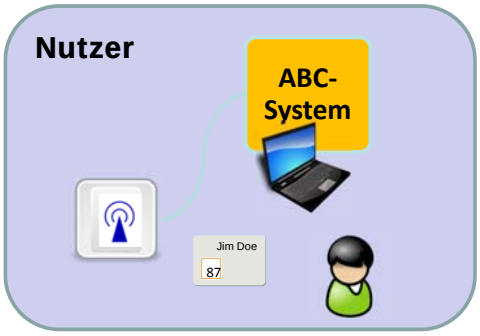
- Anwendungsanmeldung mit Karte und Lesegerät möglich
- Nur konkret erforderliche Angaben werden erfasst:
  - Anonyme Nutzung unter Nachweis bestimmter Eigenschaften, z.B. Mitglied der Schule, Alter, ...
  - Nutzung mit zum Credential verkettbaren Pseudonym zwecks Wiedererkennung, z.B. Zugriff auf unter bestimmtem Screenname verfassten Beiträgen mit Änderungsmöglichkeit, ...
  - Aufdeckbare Identität mittels Inspection (juristisch: Pseudonymität)
  - Nutzung mit verifizierter Identität (Hausaufgaben, Speicherplatz, 1:1-Kommunikation)

Umsetzung: Restricted Area Modell

- Daten und Beiträge werden in sog. Restricted Areas (RAs) abgelegt
- RAs haben bei Erstellung individuell definierte und offen einsehbare Zugriffsbedingungen
- RAs können eingesehen werden, sofern Zugriffsbedingung nachweislich erfüllt ist
- Inhalt liegt auf dem Server des Anbieters

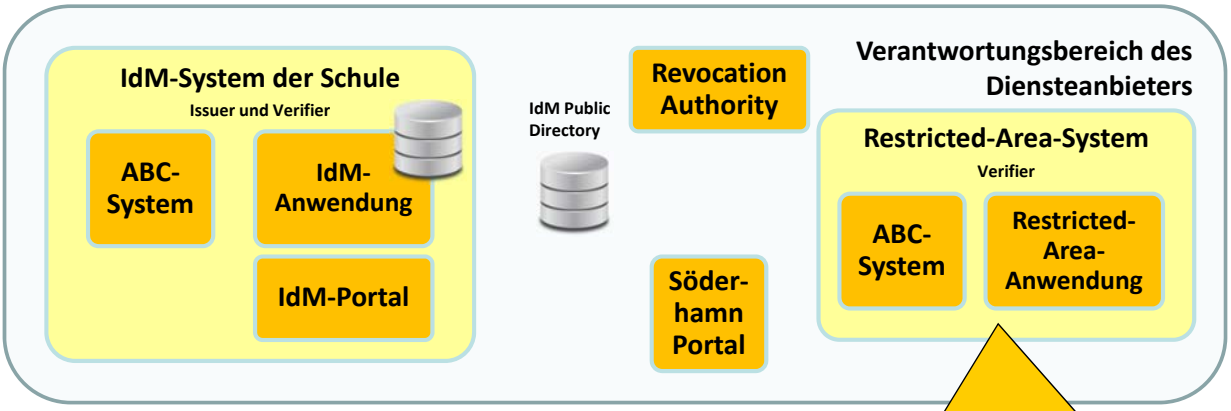
Restricted-Area-Modell

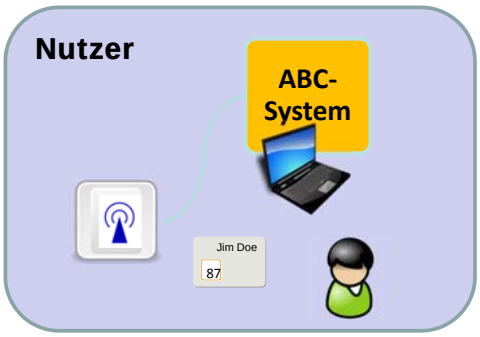




- Öffentlich zugänglicher Server mit Startseite und Links zum IdM-System, den Restricted Areas und der Revocation Authority

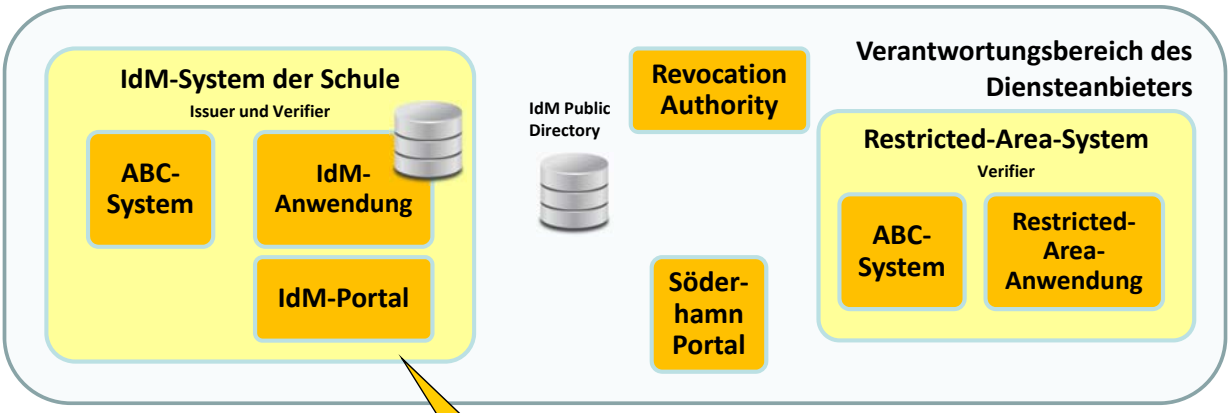
Restricted-Area-Modell

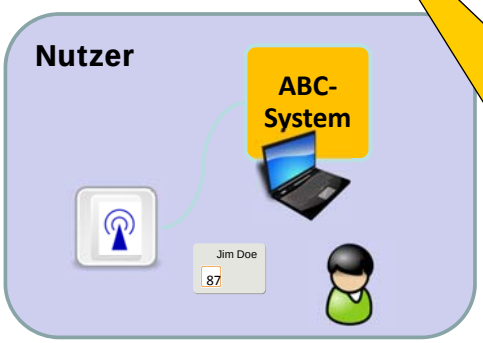




- Kern des sozialen Netzwerks
  - Inhalte sind hier abgelegt
  - ABC-System verifiziert, dass Nutzer nötige Attribute erfüllt
  - Zugang nur nach Authen-tifikation für konkrete RA möglich

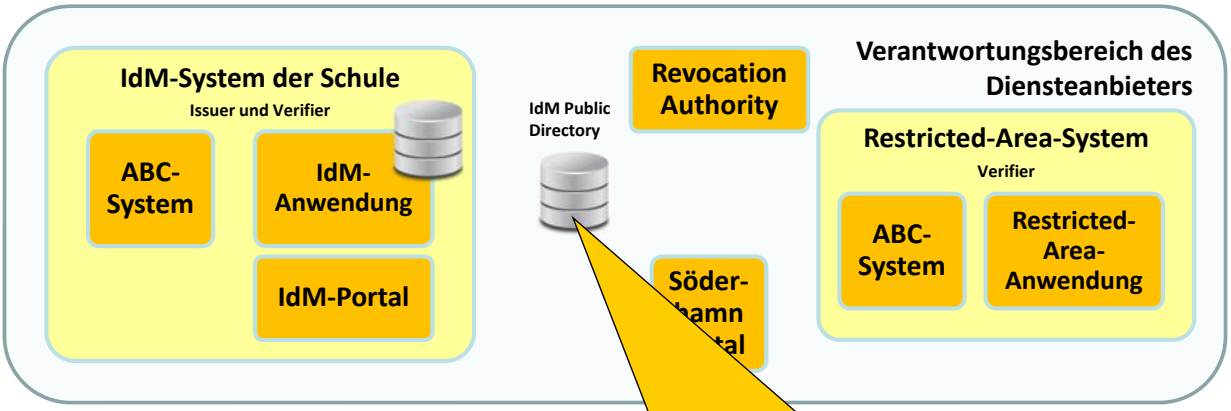
Restricted-Area-Modell

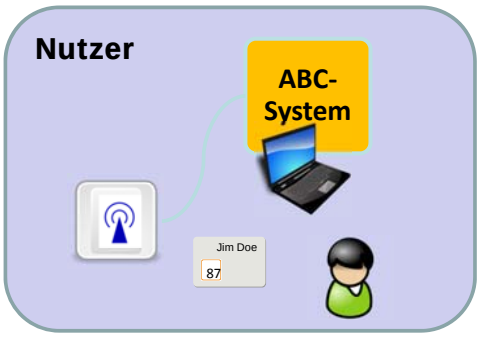




- Nutzerverwaltung der Schule
  - Erteilt Credentials (Issuer)
  - Ermöglicht Einsicht und ggf. Korrektur eigener Daten
  - Verantwortliche Stellen sind Schule und EDOC gemeinsam mit Weisungshoheit der Schule

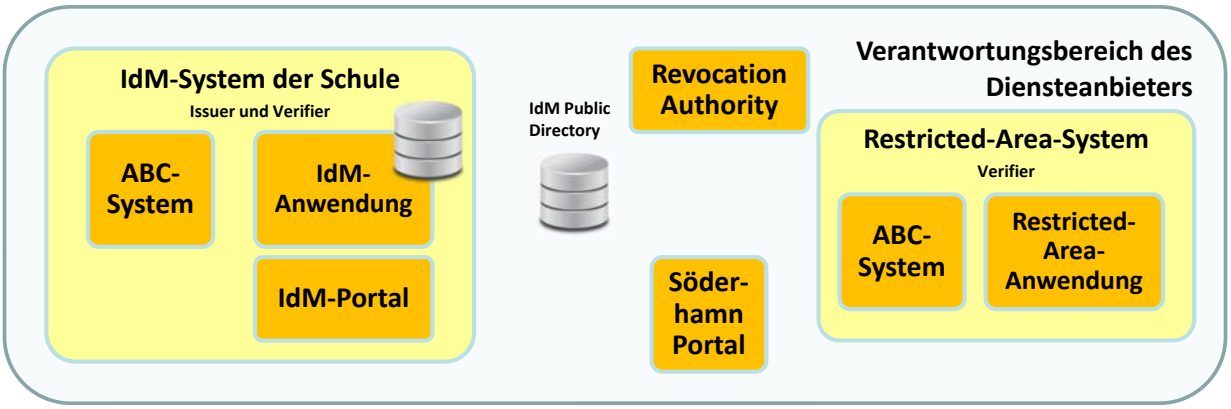
Restricted-Area-Modell

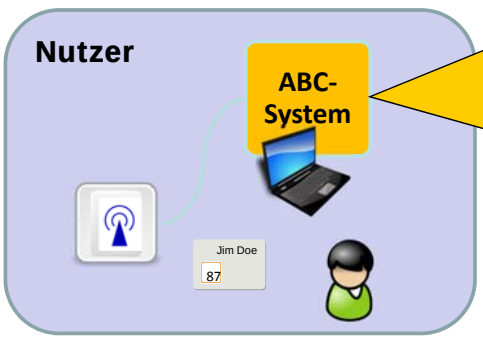




- Enthält keine personenbezogenen Daten, sondern Links zu den unterschiedlichen Diensten und Informationen über widerrufene Zertifikate (auch anonym möglich)

Restricted-Area-Modell

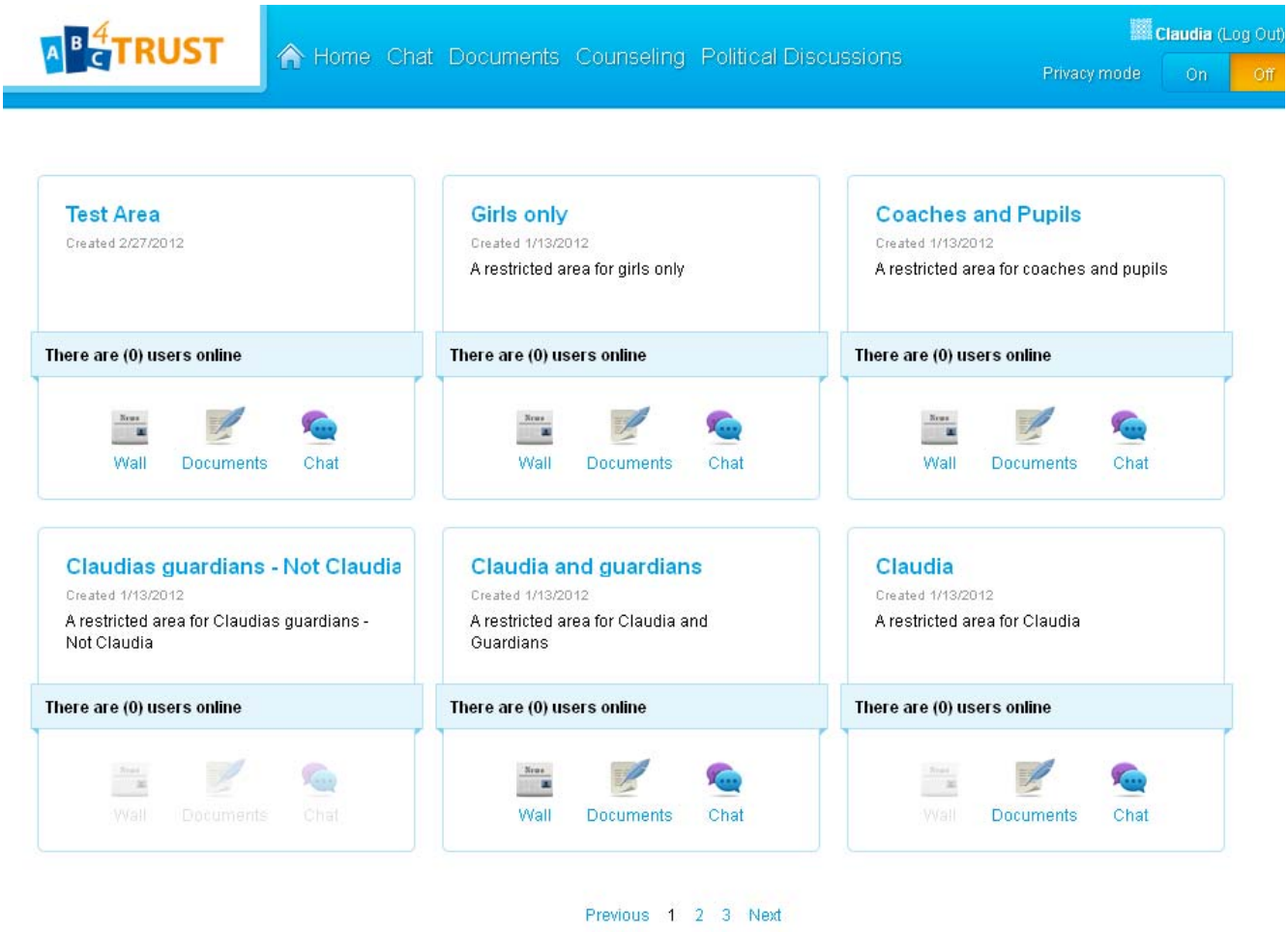




- Clientsoftware zur Unterstützung des Nutzers
- Startseite mit Übersicht der bisher besuchten RAs wird lokal erstellt, um Verkettung / Wiedererkennung zu verhindern

Umsetzung in Use Cases

- Vorgesehene Typen von Restricted Areas:
  - Eigene Dokumentenablage u.a. für Stundenpläne, Mitteilungen an Eltern, Hausaufgaben etc.
  - „Chat“ synchron oder zeitversetzt als Forum
    - Vordefinierte RAs, z.B. für Klassen, Teams, Altersgruppen
    - Selbst eröffnete RAs mit selbst definierten Anforderungen an Attribute der Nutzer
  - Politische Diskussion (anonym)
  - Chat mit Studienberater, Schulpsychologen (mit Aufdeckungsmöglichkeit soweit gesetzlich nötig und für Notfälle)



Access policy

To enter you need to reveal the following information and satisfy at least one of condition groups below.

Condition group #1

Attribute	Condition
Name	Equal to Claudia
CivicNumber	Equal to 123456-7893

Condition group #2

Attribute	Condition
Child	Equal to 123456-7893

Condition group #3

Attribute	Condition
Role	Equal to teacher

Confirm TestXml

Claudia and guardians

A restricted area for Claudia and Guardians

Wall Documents Chat

Add Favorite

Date	Description	Uploaded by	
8/17/2012 2:29 PM	Details for the swim lesson 2012. Parent's information and consent form.	Claudia	
2/28/2012 2:31 PM		teacher	Download
2/28/2012 2:31 PM		teacher	Download
2/28/2012 2:31 PM		teacher	Download
2/28/2012 2:31 PM		teacher	Download

Previous 1 Next

Online users

Claudia
0 seconds ago

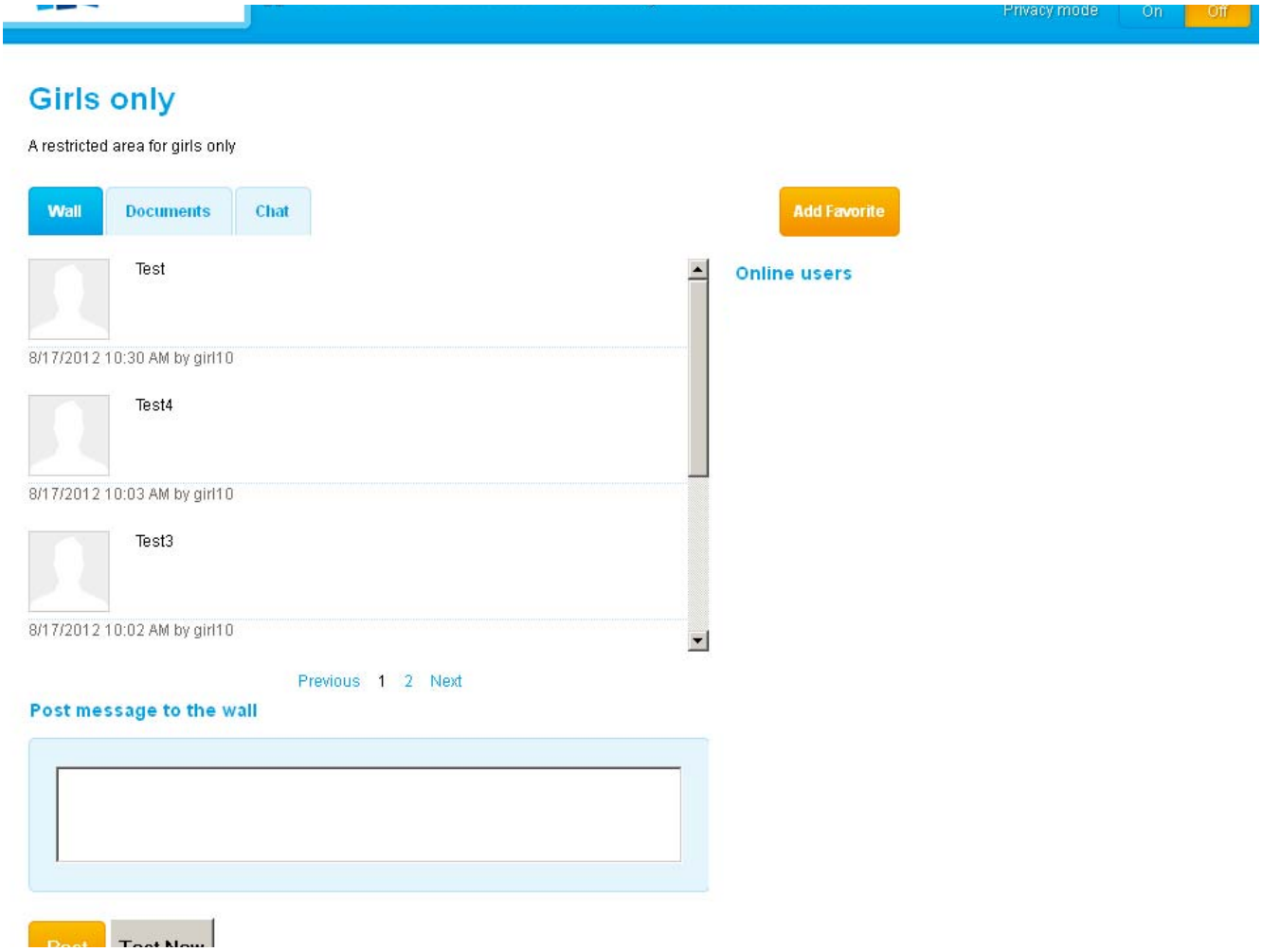
kub
Not valid ago

Upload new document

Description

Document Durchsuchen...

Upload document



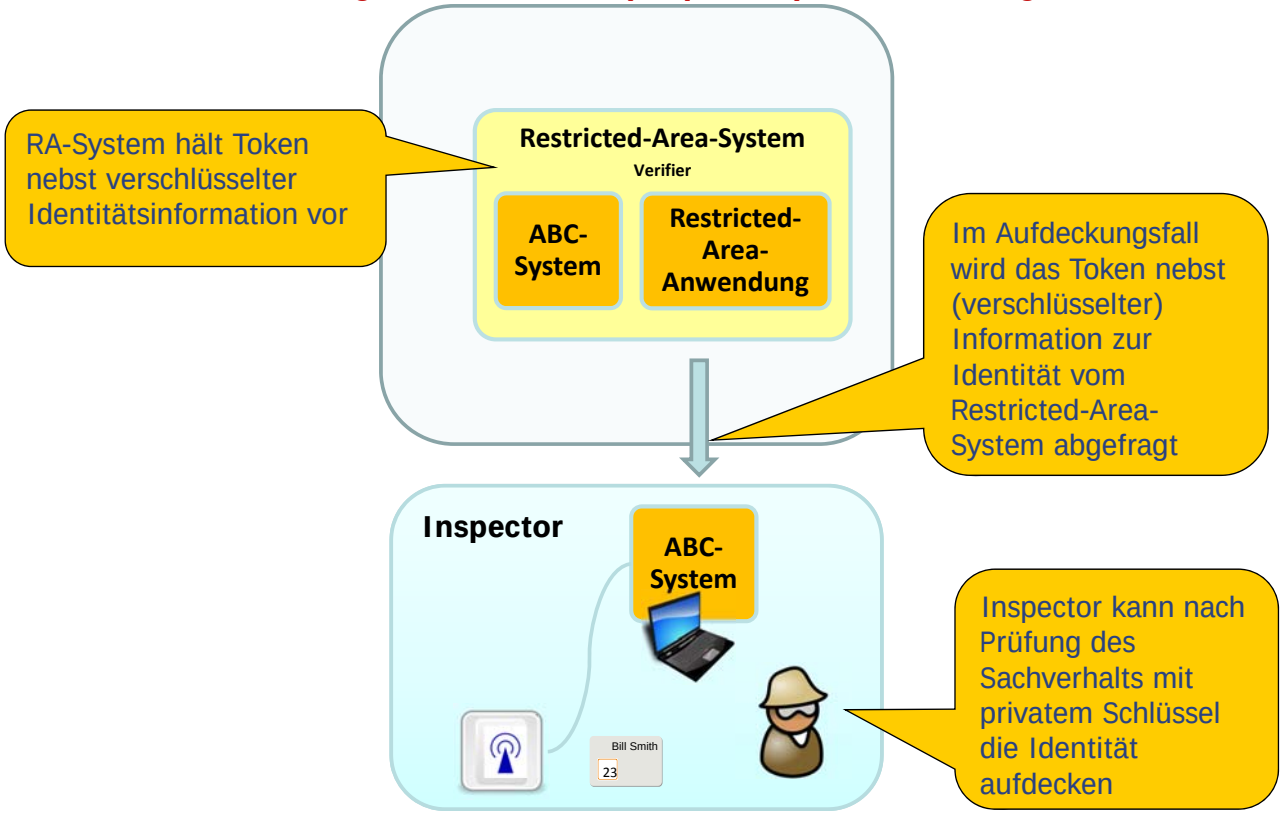
Aufdeckung von Identitäten (Inspection)

- **Problem: Volle Anonymität oft unerwünscht**
  - Misstrauen vieler Nutzer bei anonymen Teilnehmern führt zu Akzeptanzproblem
  - Haftungsrisiko für Betreiber (z.B. offener WLANs)
  - Ggf. berechtigte Interesse zur Identifikation von öffentlichen und privaten Stellen (Strafverfolgung, Finanzbehörden, Rechteverwerter, Arbeitgeber, ...)
- **Lösungsansatz: Aufdeckbare Credentials**
  - Pseudonymität bleibt im Regelbetrieb erhalten, auch gegenüber dem Betreiber und dessen Administratoren
  - Nur im vorher definierten Aufdeckungsfall ist eine Identifizierung des Nutzers möglich

Aufdeckung von Identitäten (Inspection)

- **Voraussetzungen bei Verwendung von Privacy-ABCs**
  - Anbieter des Systems verlangt Token mit verschlüsselten Angaben zur Identität des Nutzers
  - Übermittlung bedarf informierter Einwilligung vorab nebst Aufklärung über mögliche Aufdeckungsgründe, Löschfristen und Identität der Inspektoren
  - Nutzer übermittelt gewünschtes erweitertes Token
- **Anwendungsgebiete**
  - Datenminimierung mit Absicherung des Gegenübers:
    - Kreditkartendaten bei unverbindlicher Hotelbuchung,
    - Nutzung von Diensten unter Pseudonym mit Aufdeckungs-möglichkeit bei vertragswidriger Verwendung, ...

Aufdeckung von Identitäten (Inspection) im Aufdeckungsfall



Aufdeckung von Identitäten (Inspection)

Mögliche Aufdeckungsgründe (Inspection Grounds)

- Verstoß gegen zuvor klar definierte Nutzungsregeln (Upload von Pornografie, Mobbing, ...)
- Schutz von Leben und Gesundheit (Ankündigung eines Suizidversuchs oder vergleichbare Notfallsituationen)
- Gerichtliche Verfügung
- Behördliche Anordnung
- Regeln zur Vorratsdatenspeicherung (in D noch offen)
- Anbieterspezifische Regelungen (hier: schwedisches Recht z.B. mit Meldepflicht gegenüber Schulaufsicht bei Mobbing)
- ...

Aufdeckung von Identitäten (Inspection)

Aufdeckung – Problem oder Chance für Datenschutz?

- Akzeptanz datenschutzfördernder Technik kann gesteigert werden, wenn bei nachgewiesenem Bedarf eine Identitätsaufdeckung möglich ist
- Ausgleich zwischen Datensparsamkeit und Interessen Dritter bzw. sonstiger rechtlicher Anforderungen möglich
- Person bzw. Gremium des „Inspectors“ kann Rechte beider Seiten wahren (betr. Datenschutzbeauftragter)
- Umsetzung der Datentrennung auf technischer Ebene (z.B. eingeschränkter Zugriff auf Kundendaten, Aufdeckung durch internes Kontrollgremium nur bei Bedarf)

Aufdeckung von Identitäten (Inspection)

Beispiel Rechteverwertung

- EuGH: Maßnahmen zum Schutz der Inhaber von Urherberrechten müssen ein „angemessenes Gleichgewicht zwischen dem Schutz dieses Rechts und dem Schutz der Grundrechte von Personen, die von solchen Maßnahmen betroffen sind," sicherstellen.[1)]
  - Nutzer bleiben unerkannt bis zur Aufdeckung
  - Nicht-Verkettbarkeit zu anderen Beiträgen des Nutzers
  - Inspector prüft Berechtigung bzw. Plausibilität einer externen Anfrage[2)]
  - Inspector stellt Transparenz durch Mitteilung sicher

[1)] EuGH C-360/10 - SABAM vs. Netlog, Rz. 43, mit Verweis auf C-275/06 - Promisicae
[2)] Vergl. zu Behördenanfragen *Kamp*, RDV 2007, 236, 238; Schmidt, ZD 2012, 63, 64.

Einzelfragen

Zugriffe von Eltern

- Zugriffe von Eltern auf Beiträge ihrer Kinder sind grundsätzlich nicht vorgesehen; eine Einsicht wäre nur mit dem Kind gemeinsam unter Nutzung der Credentials des Kindes möglich

Möglichkeiten zur Erweiterung

Vollverschlüsselung der Inhalte

z.B. mit „Scramble!“ aus dem Projekt PrimeLife:
http://primelife.ercim.eu/results/opensource/65-scramble

- Nachteil: Beitretende zu einer Gruppe können ältere Kommentare mangels Schlüssels nicht lesen
- Umfassende Public-Key-Infrastruktur fehlt
- Verschlüsselung an bestimmte Empfänger erlaubt womöglich Identifikation des Empfängers

⇒ Schutz der Inhalte gegenüber dem Betreiber durch Vollverschlüsselung und Funktionalität als soziales Netzwerk schließen sich aus

Möglichkeiten zur Erweiterung

Anonymitäts-Level anzeigen

- Verkettung oder Identifikation eines Nutzers theoretisch möglich, wenn die infrage kommende Gruppe (Anonymitäts-Set) zu klein ist (z.B. nur ein schachspielender Lateinschüler im Fußballteam)
- Ermittlung des Anonymitäts-Levels ist nur denkbar mit Zugriff auf die Nutzerdatenbank
- Bloße Statistik zu allen Gruppen genügt nicht, da Umfang der Überschneidungen unbekannt ist

⇒ Nutzern könnte es helfen, beim Erstellen oder Betreten einer Restricted Area die Größe der Gruppen mitgeteilt zu bekommen

Möglichkeiten zur Erweiterung

Alternative Zugangsmethoden

- Neue Verschlüsselungsverfahren mit ähnlichem Funktionsumfang können mit der in ABC4Trust entwickelten Protokollebene verwendet werden.

- Andere anonyme Methoden zur Authentifizierung (z.B. neuer Personalausweis) könnten auf Anwendungsebene eingebunden werden.

Fragen? Anregungen?

Kontakt:
Harald Zwingelberg
abc4trust@datenschutzzentrum.de
www.datenschutzzentrum.de
0431/988-1228

und hinsichtlich
ABC4TRUST
unter: www.abc4trust.eu

High Level Architecture / Söderhamn Pilot (cont. 8)
Inspection