Einfluss neuer Cookie-Richtlinien auf SSO und SLO

ssystems GmbH | Berlin und München | 28.03.2023

Agenda

1. 3rd Party Cookies - Tracking
2. Cookies im Detail
3. Google Privacy Sandbox
4. SSO und SLO Auswirkungen
5. Hands On

Firmengeschichte

Gegründet im Jahr 2003 verfügt ssystems über 20 Jahre Erfahrung in der Zusammenarbeit mit Personen, Gruppen, Teams in Hochschulen, die sich mit Campus-IT beschäftigen.

ssystems mit seinen Sitzen in München und Berlin ist derzeit eines der wenigen Unternehmen in Deutschland, die mit den Herausforderungen von Campus-IT auch im Kontext großer Hochschulen vertraut sind und bei dem das konzeptionelle und technische Fachwissen existiert, um ihre Projekt kompetent begleiten zu können.

Wir sind groß genug, um komplexe Lösungen realisieren zu können und dabei menschlich präsent und organisatorisch flexibel sind.

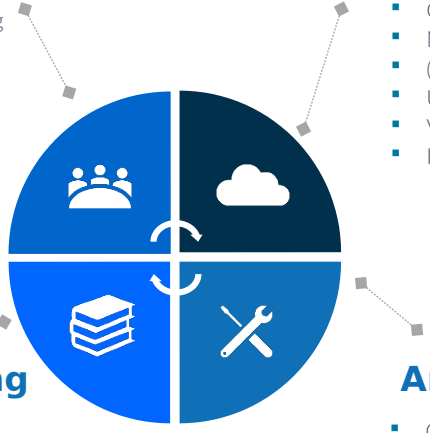
Über uns

Umfassende, professionelle IT-Serviceleistungen

Identity und Access Management

- Beratung, Konzeption und Umsetzung
- Erweiterung und Integration
- Verwaltung und Betrieb
- Metadirectories und Prozessberatung
- Verzeichnisdienste
- SSO, SAML, Shibboleth und AAI
- OAuth, OpenID Connect,...

Shibboleth OpenID Connect



Server und Infrastruktur

- Campus Management, LMS, ..
- Mail, Web, Storage
- (Managed) Hosting IaaS
- UNIX, Linux und Netzwerke
- Virtualisierung
- IT Security und Datenschutz

Hosted in Germany

E-Learning, E-Prüfung

- Moodle, Blackboard, CLIX, Opencast
- Social Learning, E-Portfolios, Mahara
- Online Klausuren – E-Assessment
- CMS: TYPO3, Drupal, Firstspirit, WordPress

OPENCAST moodle

Anwendungsentwicklung

- CMS und LMS Erweiterungen
- Systemprogrammierung, Backends
- Customized Frontends
- JAVA, Spring, GWT, NodeJS,..
- Python, PHP, Shell, uvm.

ssystems

Einige Referenzen

Nachhaltige Dienstleistungen

virtuelle hochschule bayern
Bauhaus-Universität Weimar
JKU JOHANNES KEPLER UNIVERSITÄT LINZ
Julius-Maximilians-UNIVERSITÄT WÜRZBURG
EBERHARD KARLS UNIVERSITÄT TÜBINGEN
HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN · FH MÜNCHEN
SIMOVATIVE Campus Management Software
iu INTERNATIONALE HOCHSCHULE
HNU HOCHSCHULE NEU-ULM UNIVERSITY OF APPLIED SCIENCES
HOCHSCHULE ANSBACH
SFU Sigmund Freud PrivatUniversität Wien
UNIVERSITÄT PADERBORN
Evangelische Hochschule Nürnberg
UNIVERSITY OF BAMBERG OTTO-FRIEDRICH-UNIVERSITÄT BAMBERG
Hochschule Kempten University of Applied Sciences
hochschule aschaffenburg university of applied sciences
ssystems

Motivation

Das Spannungfeld zwicschen Usability, Security und Compliance

Phase out von 3rd party cookies

Change in Progress: Identifikation, Sessions, Federation und Tracking

Gesetzliche Vorgaben

DSGVO: Datensparsamkeit, Informationelle Selbstbestimmung, Cookie-Richtlinie

Sicherheit

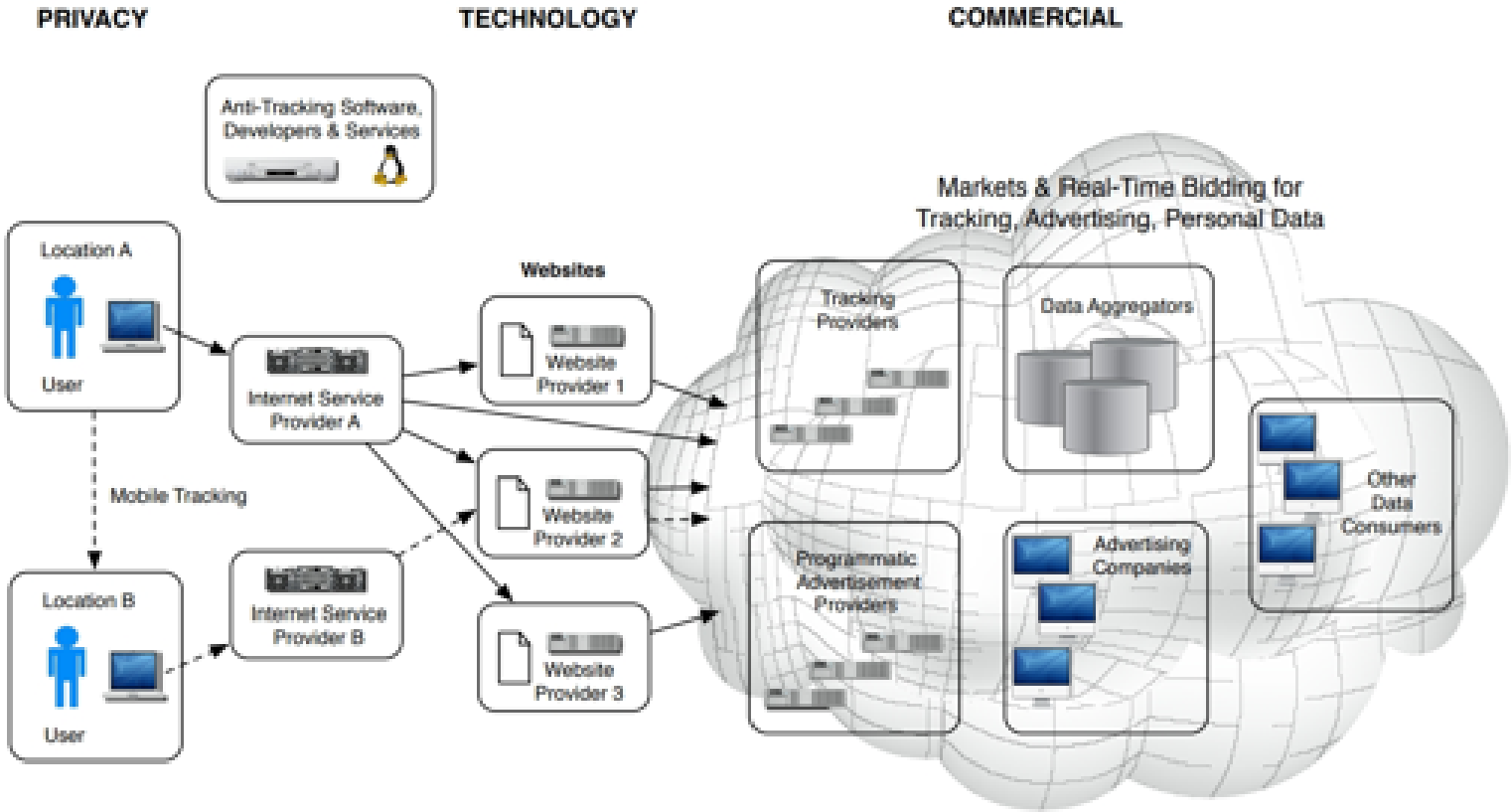
Cloudless, Seperation Of Duties, MFA, Single Logout, Best Practice

Usability

Einfache Logins, SSO, Autom. Datenweitergabe, Erweiterbarkeit, WebAuthN, etc,

?

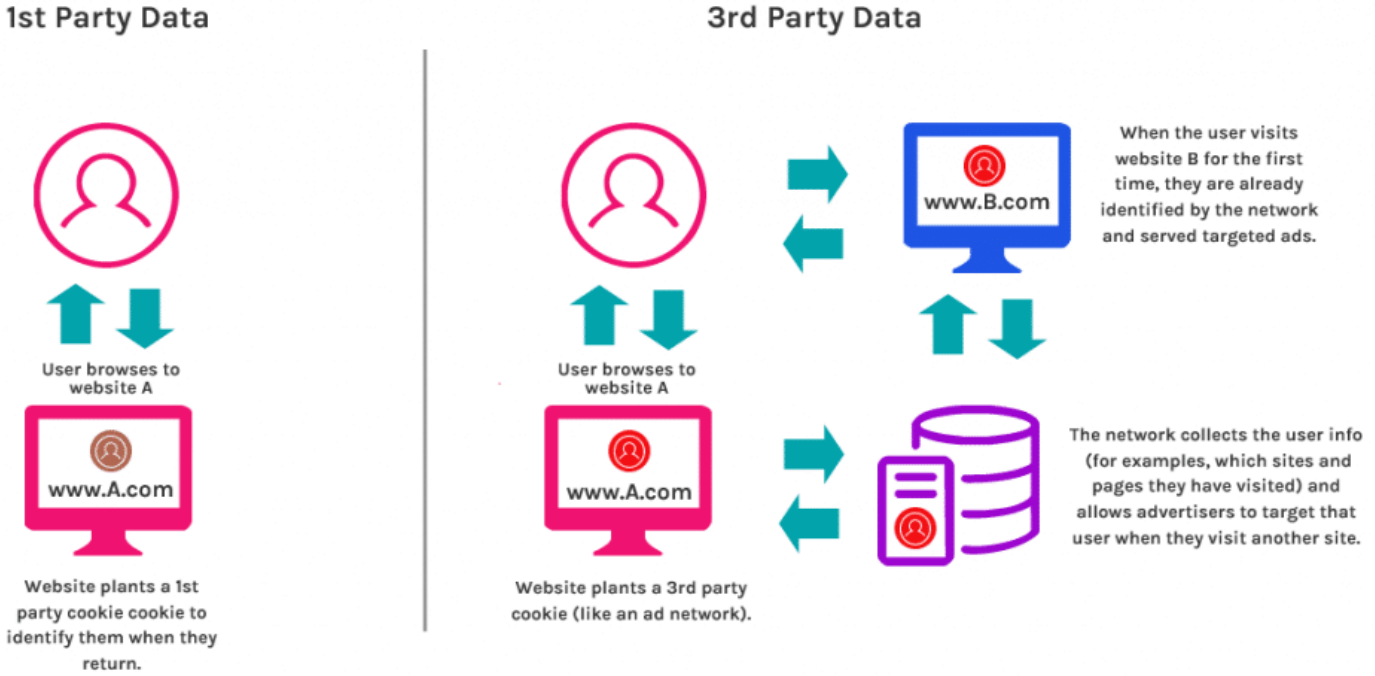
Web Tracking



Quelle: Ermakova, Tatiana & Fabian, Benjamin & Bender, Benedict & Klimek, Kerstin. (2018). Web Tracking – A Literature Review on the State of Research. 10.24251/HICSS.2018.596.

3rd Party Cookies

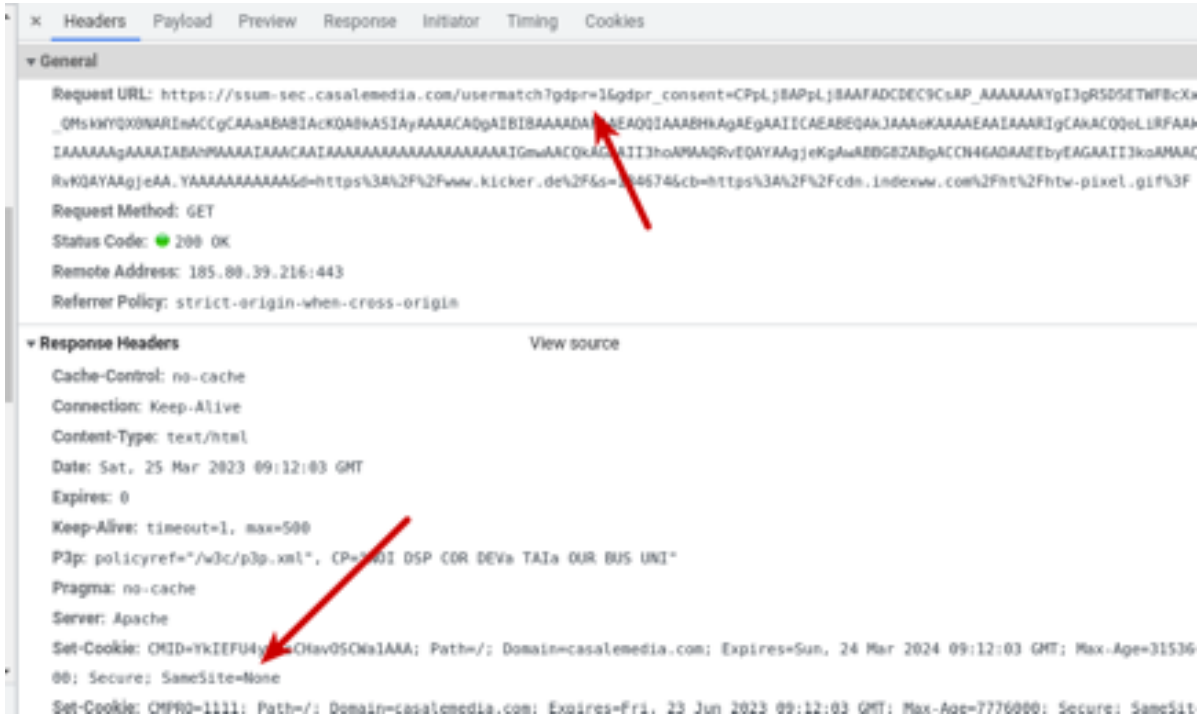
Zugriffe im Hintergrund



Quelle: https://www.singlegrain.com/advertising/privacy-sandbox/

EU Cookie-Richtlinie

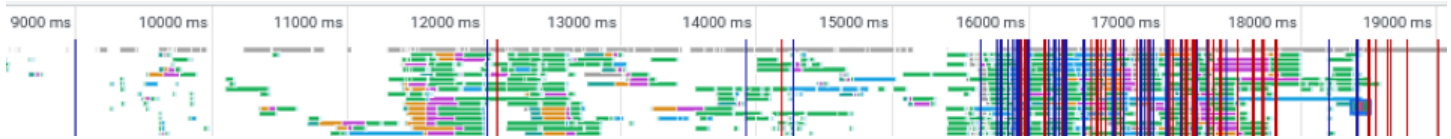
IFRAME, IMG, JS, ...



Quantitative Betrachtung

Anteil der Tracking- und AD-Requests > Inhalte

Chrome Browser



Brave Browser

Quelle: https://crackedlabs.org/en/corporate-surveillance

Qualitative Betrachtung

Schützenswerte Attribute

Quelle: https://crackedlabs.org/en/corporate-surveillance

Cookies, Cloud und Big Data

How the Internet should look like and how it looks like...

These Algorithmen arbeiten im Hintergrund. Bias Detection wird so gut wie nicht umgesetzt, Bürokratie erschwert schnelle Änderungen

Dr. Paul Vixie
Oportunistic abuse of internet protocols

Machine Learning und Bias
Algorithmen sind sehr gut darin, zwischen den Zeilen zu lesen.

Dr. Sandra Wachter: Unfair AI
Aus technischen Problemen sind soziale Probleme entstanden: Jobs, Kredite, etc.

Kein Ende des Trackings
Browser Fingerprinting, Local Storage, Indexed DB,...

Basisrate
2017 Acxiom provided its clients with **3,000 attributes** on 700 million people. Just one year later that number was up to **10,000 attributes on 2.5 billion people**

vgl: https://rudolphina.univie.ac.at/internetforschung-wie-algorithmen-unser-leben-veraendern

Exkurse

Cookies und Googl Privacy Sandbox

Florian Rittherhoff

Deep Dive in technische Aspekte von Cookies

Michael Fuchs

Google Privacy Sandbox

Cookies, Privacy Sandbox und seine Auswirkungen

Hochschule für angewandte Wissenschaften München

Florian Ritterhoff & Michael Fuchs

28. März 2023

Grundlagen

- Setzen und Lesen prinzipiell entweder via HTTP-Header oder via JavaScript möglich

- HTTP-Header
  - Server Response: `Set-Cookie: foo=bar`
  - Client Request: `Cookie: foo=bar`
- Zugriff auf Set-Cookie Header durch JavaScript in der Regel nicht möglich (*Forbidden*-Header)

- JavaScript
  - `document.cookie = "foo=bar"`

HttpOnly

- Einschränkung der Zugriff mittels JavaScript
- Cookies mit HttpOnly Header sind durch JavaScript nicht lesbar, werden jedoch weiterhin bei `fetch` Anfragen übermittelt.

Expires & Max-Age

- Definiert maximale Lebensdauer eines Cookies bzw. kann auch dazu verwendet werden, ein Cookie zu invalidieren
- `Max-Age`: Lebenzeit in Sekunden
- `Expires`: Zeitstempel für Invalidierung

- Möglichkeit zum ”Löschen”mit altem Zeitstempel

Secure

- Einschränkung der Übermittlung auf ausschließlich https
- Ausnahme: localhost

Domain

- Spezifikation einer Domain, für die Cookie übermittelt wird
- Möglich nur aktuelle Domain oder übergeordnete Domains
- Umfasst bei Verwendung alle Subdomains
  Ohne Definition lediglich die Originalseite

Path

- Analog zu Domain Spezifikation - Konfiguration von gültigen Pfaden und den dazugehörgen Unterordnern

SameSite

- Unterscheidung zwischen First-Party Cookie oder Third-Party Cookies
- Auswirkungen auf die Übermittlung bei verschiedenen Anfragen (Cross-Site)
  $\Rightarrow$ Schutz vor Cross-Site-Request-Forgery
- Mögliche Werte:
  - `None`
    Übermittlung bei allen Anfragen
  - `Strict` Übermittlung ausschließlich zu „Same-Site” Seiten
  - `Lax`
    Übermittlung zu „Same-Site” + wenige sichere HTTP Methoden (GET, HEAD, OPTIONS und TRACE)

Exkurs: First-Party vs. Third-Party Cookies

- Normalerweise Cookie verknüpft mit Domain und Schema (http/https) und optional gültig für Subdomains

- Einbindung von externen Ressourcen: Berücksichtigung der `Site`
- `Site`: Public Suffix + 1 $\rightarrow$ d.h. i.d.R. Top Level Domain + Erster Domainname
- Public Suffix List umfasst aber auch Dienste wie `github.io`
- Cross Site $\Rightarrow$ Einbindung von Informationen von externen Seiten („andere Site")

SameSite

- Standardwert in der Regel Lax, jedoch abhängig von Browser Version (u.a. Firefox und Safari verwenden `None`)
- `SameSite=None` erfordert i.d.R. `Secure` Flag

First Party Sets - *Proposal*

- Erweiterung d. SameSite Funktionalität um Zusammenfassung von verschiedenen Websiten zu einer Gruppe
- Chrome und Safari wollen es implementieren bzw. haben es bereits implementiert
- Firefox/Brave/... weigern sich bislang
- Spezifikation von mehreren „verwandten“ Seiten auf Hauptdomain und Verweis von weiteren Seiten auf genau eine Hautpdomain

First Party Sets - *Proposal*

Beispiel:

- Hauptdomain: hm.edu
- Verwandte Domains: fh-muenchen.de, muas.de, hm.education, ...

- SameSite=Strict → Übermittlung von Cookies nur an hm.edu bei hm.edu Seiten
- Verwendung von FPS ermöglicht „umgehen" dieser Beschränkung

Demonstration von verschiedenen SameSite Einstellungen

Big Picture

- von Google geleitete Initiative von Unternehmen und Organisationen
- standardisierter Zugriff auf Nutzerdaten ohne Gefährdung der Privatspähre
- Hauptzweck: Online-Werbung ohne third-party Cookies
- Projekte der Privacy Sandbox seit 08/2019 in Entwicklung
- Forschungsprojekte: *Federated Learning of Cohorts*
- Initiative ist wettbewerbswidrig mit kartellrechtlichen Reaktionen

Primäre Ziele

- Ersetzen der Funktionalität des Cross-Site-Trackings
- Entfernen von Cookies von Drittanbietern
- Abschwächen des Risikos des Fingerprinting von Geräten
- (gezielte) Werbung nur noch über Technologien der Privacy Sandbox möglich!

Sekundäre Ziele

- Schützen der Privatsphäre aller Menschen im Internet
- Entwicklungszwerkzeuge, um florierende digitale Unternehmen aufzubauen
- native Unterstützung im Web sowie Android
- **Nebeneffekt**: Online-Inhalte und -Dienste sollen kostenlos bleiben

Architektur

- Vorschläge der Privacy Sandbox basieren auf Werbung
- Webbrowser kontrolliert Privatsphäre des Nutzeres
- Werbung ist nicht mehr an Einzelpersonen sondern an Kohorten gerichtet
- Datenerfassung und -verarbeitung wird auf Gerät des Nutzenden verlagert

Honi soit qui mal y pense: Verteilung der Marktanteile von Browsern?

What about W3C?

- seit 01/2022 laut Google Beteiligung von Werbeunternehmen in der *Improving Web Advertising Business Group (IWABG)* erwünscht
- W3C ist konsensbildende Organisation
- Technologien können trotzdem ohne Konsenz eingesetzt werden

Deep Dive

- Blockierung von aktuellen Tracking-Mechanismen und Fingerprinting
- Bereitstellung von datenschutzfreundlicher Werbung
- Zusammenarbeit mit Industrie, Publisher, Entwickler, Werbetreibende und anderen Personen
- Datenschutzstandards für Web und Android
- Open-Source

Exkurs: Konzepte von Chrome

- Shipped
- In beta
- Origin Trials, u. a. für URLs
- Developer Trials
- No longer persuing

Grundsätzlich kann das *Features Flag* aktiviert werden!

Timeline: Overview

Timeline: Launched

- **SameSite Cookies**: Explizites Kennzeichnen von seitenübergreifender Cookies
- **User-Agent Client Hints API**: Umstellung des User-Agent String auf User-Agent Client Hinweise, wie z.B. `Accept-CH: Sec-CH-UA-Model` sowie `Sec-CH-UA-Model: "Pixel 5"`
- **HTTP Cache Partitioning**: Partitionierung des HTTP-Cache von Chrome
- **DNS-over-HTTPS auto-upgrade**: RFC 8484 DNS Queries over HTTPS (DoH)

Timeline: In Development

- **Network State Partitioning**: HTTP-Cache (Chrome) pro Website anstatt globales Handling. Transitive Teilhabe am *fetch*-Standard
- **User-Agent Reduction**: Begrenzung passiv freigegebener Browserdaten zur Verminderung des Fingerprinting
- **Storage Partitioning**: Teilhabe an der *Client-Side Storage Partitioning Working Group* der *Privacy Community Group*

Timeline: Early phases

- **IP Protection**: Verbesserung der Privatsphäre indem die IP-Adresse nicht mehr zur Nachverfolgung verwendet wird
- **Privacy Budget**: Begrenzung der individuellen Nutzerdaten auf Websites zur Verhinderung verdeckter Nachverfolgung
- **Bounce Tracking Mitigations**: Reduktion bzw. Eleminierung des kontextübergreifendes Tracking (Bounce Tracking)

Konzepte - Web I

- Bekämpfung von Spam und Betrug im Internet
  - **Private State Tokens**: verschlüsselte, kontextübergreifende Token zur Unterscheidung zwischen Personen und Bots
- Anzeige relevanter Inhalte und Anzeigen
  - **Topcis API**: Spezifizierung und explizite Freigabe von besuchten Websiten durch Browser
  - **FLoC API**: Zusammenfassung von Personen mit ähnlichen Surfverhalten in Kohorten
  - **FLEDGE**: Remarketing ohne Zugriff auf Cookies auf Drittanbietern

Konzepte - Web II

- Stärkung der Grenzen des gegenseitigen Vertrauens
  - **First Party Sets**: Einschränkung des Informationsaustausch auf vordefinierte Domänen
  - **Shared Storage API**: Sicheres Teilen eines gemeinsamen Speichers im Browser für unterschiedliche Single-Page-Applications
  - **CHIPS (Cookies Having Independent Partitioned State)**: Einführung von partitionierten Cookies für Websites innerhalb des First Party Sets
  - **Fenced Frames API**: eingebetteter *iframe*, welcher nicht mit der Host-Seite kommunzieren kann und jeweils mit Hauptseite identifiziert ist
  - **Federated Credential Management API**: Handling von föderierten Identitätskonzepte, welche auf Cookies von Drittanbietern beruhen
  - **Storage Partitioning** und **Network State Partitioning**

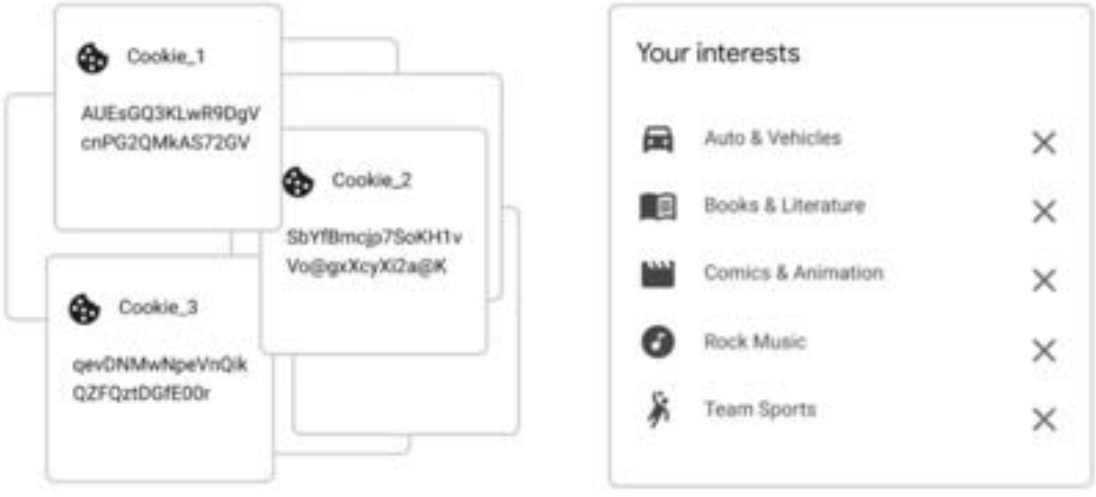
Konzepte - Web III

- Messung digitaler Anzeigen
  - **Attribution Reporting API**: Mess- und Berichterstattungsinstrumente für das Surverhalten von Personen und deren Reaktion auf Werbung
- Limit von geteiliten Informationen
  - **Same-Site Cookies**, **User-Agent Client Hints**, **User-Agent Reduction**, **HTTP Cache Partitioning**, **DNS-over-HTTPS**, **IP Protection** und **Privacy Budget**

Konzepte - Android

- Anzeige relevanter Inhalte und Anzeigen
  - **Topcis API** und **FLEDGE**
- Messung digitaler Werbung
  - **Attribution Reporting**: Tracking-Methodiken, wie z.B. Advertising ID, sollen nicht mehr auf Nutzerbasis basieren
- Limit von geteiliten Informationen
  - **SDK Runtime**: isolierter Prozess für Code von Drittanbietern, sodass Nutzerdaten und Werbung getrennt sind

Topics API I

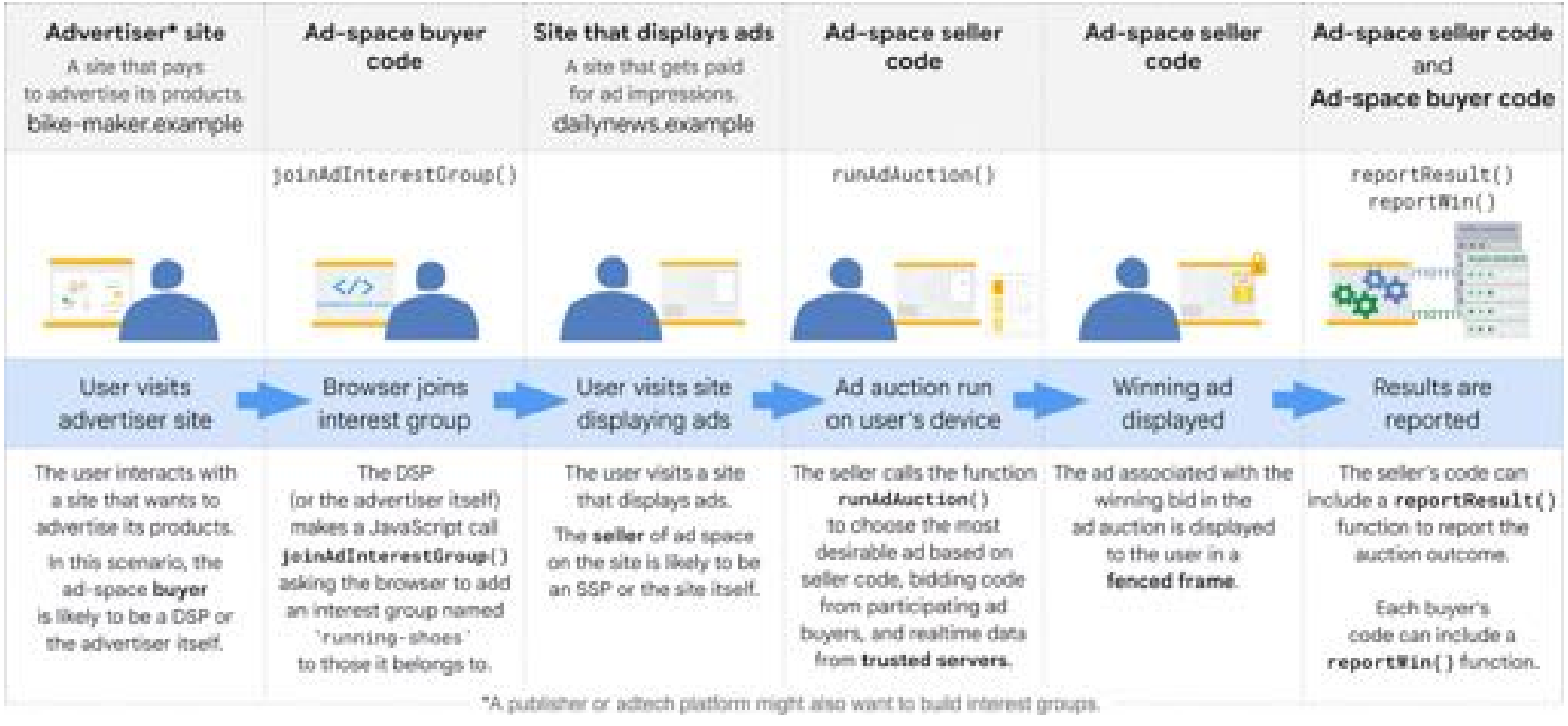

Cookie_1
AUEsGQ3KLwR9DgV
cnPG2QMkAS72GV
Cookie_2
SbYfBmcjp7SoKH1v
Vo@gxXcyXi2a@K
Cookie_3
qevDNMwNpeVnQik
QZFQztDGfE00r
Your interests
Auto & Vehicles
Books & Literature
Comics & Animation
Rock Music
Team Sports

Topics API II

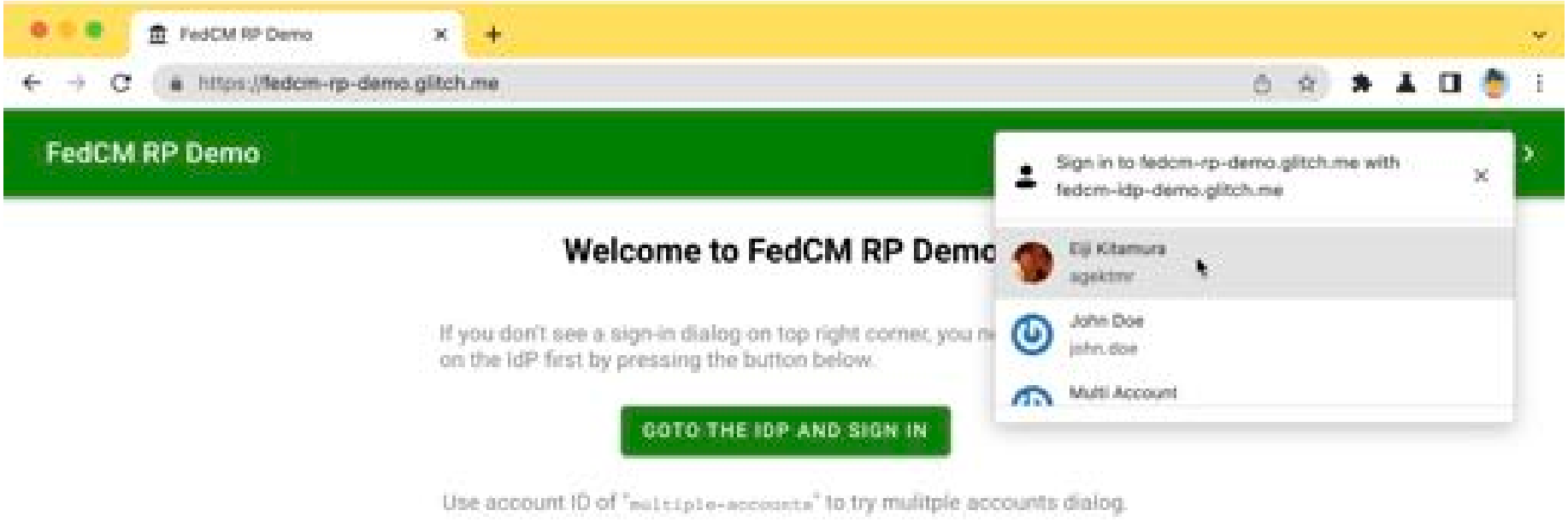
Topcis API - III

- große Player aka. Google werden bevorzugt
- User-Experience ist nicht transparent bzw. schwierig zu bedienen
- Ist User-Profiling mit Machine Learning möglich?
- Datenschutzfreundliche Default-Settings in Chrome?
- *Trade-off]*: Security/Datenschutz vs. Bequemlichkeit des Nutzenden

FLEDGE


Advertiser* site
A site that pays to advertise its products.
bike-maker.example
Ad-space buyer code
joinAdInterestGroup()
Site that displays ads
A site that gets paid for ad impressions.
dailynews.example
Ad-space seller code
runAdAuction()
Ad-space seller code
Ad-space seller code and Ad-space buyer code
reportResult()
reportWin()
User visits advertiser site
Browser joins interest group
User visits site displaying ads
Ad auction run on user's device
Winning ad displayed
Results are reported
The user interacts with a site that wants to advertise its products.
In this scenario, the ad-space buyer is likely to be a DSP or the advertiser itself.
The DSP (or the advertiser itself) makes a JavaScript call joinAdInterestGroup() asking the browser to add an interest group named 'running-shoes' to those it belongs to.
The user visits a site that displays ads.
The seller of ad space on the site is likely to be an SSP or the site itself.
The seller calls the function runAdAuction() to choose the most desirable ad based on seller code, bidding code from participating ad buyers, and realtime data from trusted servers.
The ad associated with the winning bid in the ad auction is displayed to the user in a fenced frame.
The seller's code can include a reportResult() function to report the auction outcome.
Each buyer's code can include a reportWin() function.
*A publisher or adtech platform might also want to build interest groups.

Federated Credential Management API (FedCM) - I



Federated Credential Management API (FedCM) - II

- Unfortunately, the *mechanisms that identity federation* has relied on (iframes, redirects and cookies) are *actively being abused to track users* across the web. As the *user agent isn't able to differentiate* between identity federation and tracking, the *mitigations* for the various types of abuse make the *deployment of identity federation more difficult*.
- Enterprises and Education: As is clear at the FedID CG, there are still a *lot of use cases* that *FedCM does not well serve* that we'd like to work on, such as *front-channel logout* (the ability for an IdP to send a signal to RPs to logout) and *support for SAML*.

Federated Credential Management API (FedCM) - III

- Kein Support für Front Channel Single-Sign-Out
- Kein Support für SAML
- Identity Federation wird schwieriger

Weitere Informationen

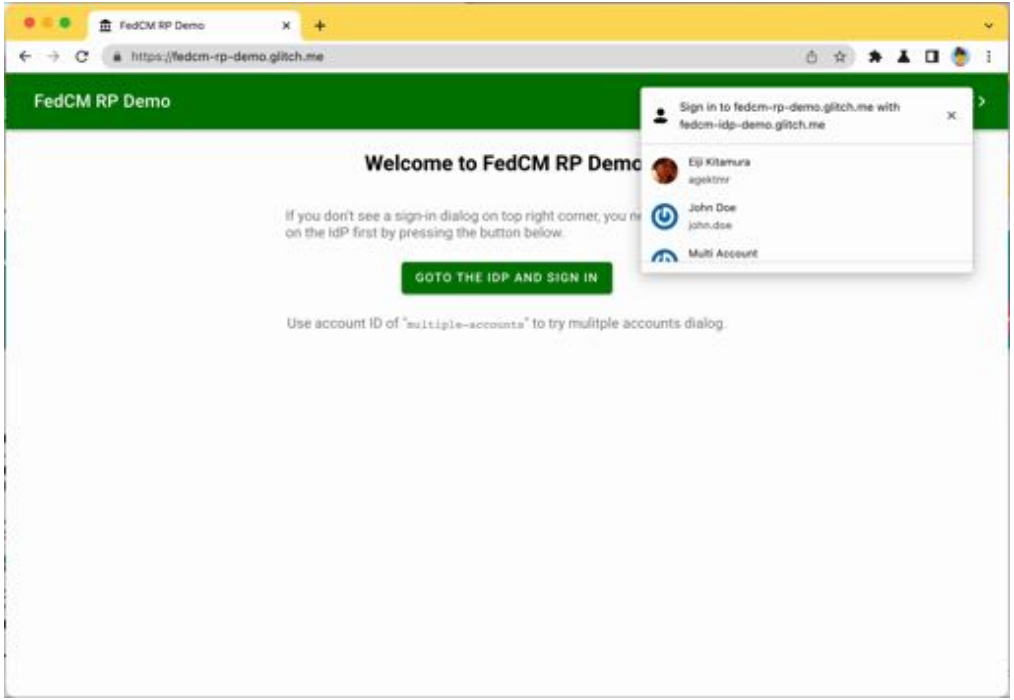
- https://privacysandbox.com/
- https://privacysandbox.com/learning-hub/
- https://web.dev/digging-into-the-privacy-sandbox/
- https://www.chromium.org/Home/chromium-privacy/privacy-sandbox/
- https://developer.android.com/design-for-safety/privacy-sandbox
- https://blog.google/products/android/introducing-privacy-sandbox-android/

Vielen Dank für die Aufmerksamkeit!

Fragen?

FedCM

Federated Credential Management API



Quelle: https://developer.chrome.com/docs/privacy-sandbox/fedcm/

FedCM II

Noch nicht ausgereift

FedCM Shortcomings

- the **user agent isn't able to differentiate between identity federation and tracking**, the mitigations for the various types of abuse make the deployment of identity federation more difficult.
- Enterprises and Education: As is clear at the FedID CG, **there are still a lot of use cases that are not well served by FedCM** that we'd like to work on, such as front-channel logout (the ability for an IdP to send a signal to RPs to logout) and support for SAML

Geplant: cross-origin Iframe support

Aktuell keine Unterstützung von SAML

Aktuell kein Front Channel SLO

vgl. https://developer.chrome.com/docs/privacy-sandbox/fedcm/

SameSite Cookies und SPs

Im Normalfall sind Flows in Top Level Navigation umgesetzt

Aspekte im Zusammenhang mit Service Providern, die vom Phase-out von 3rd Party Cookies betroffen sind:

- SP setzt sameSite=None
- Alter Safari Bug: sameSiteFallback=true
- Anpassungen ggf. kontextbezogen an Anwendungen notwendig

Top-level navigation bei normalen SSO, kein Problem

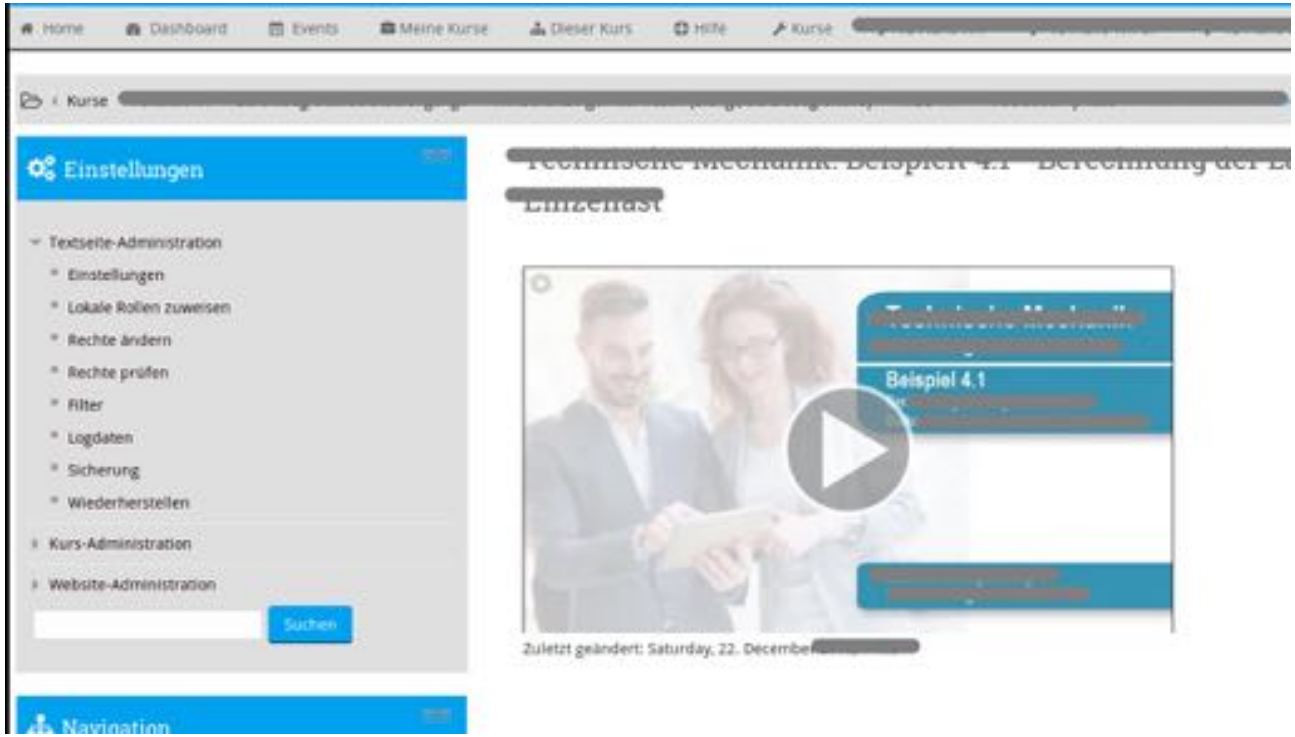
Requests aus Iframes bei SLO, teilweise ein Problem

Problem bei Iframes mit SSO Auth.

vgl. https://shibboleth.atlassian.net/wiki/spaces/SP3/pages/2093318581/SameSite

Embedding von Videos

Autorisierung bei aktivem Top Level SSO Kontext

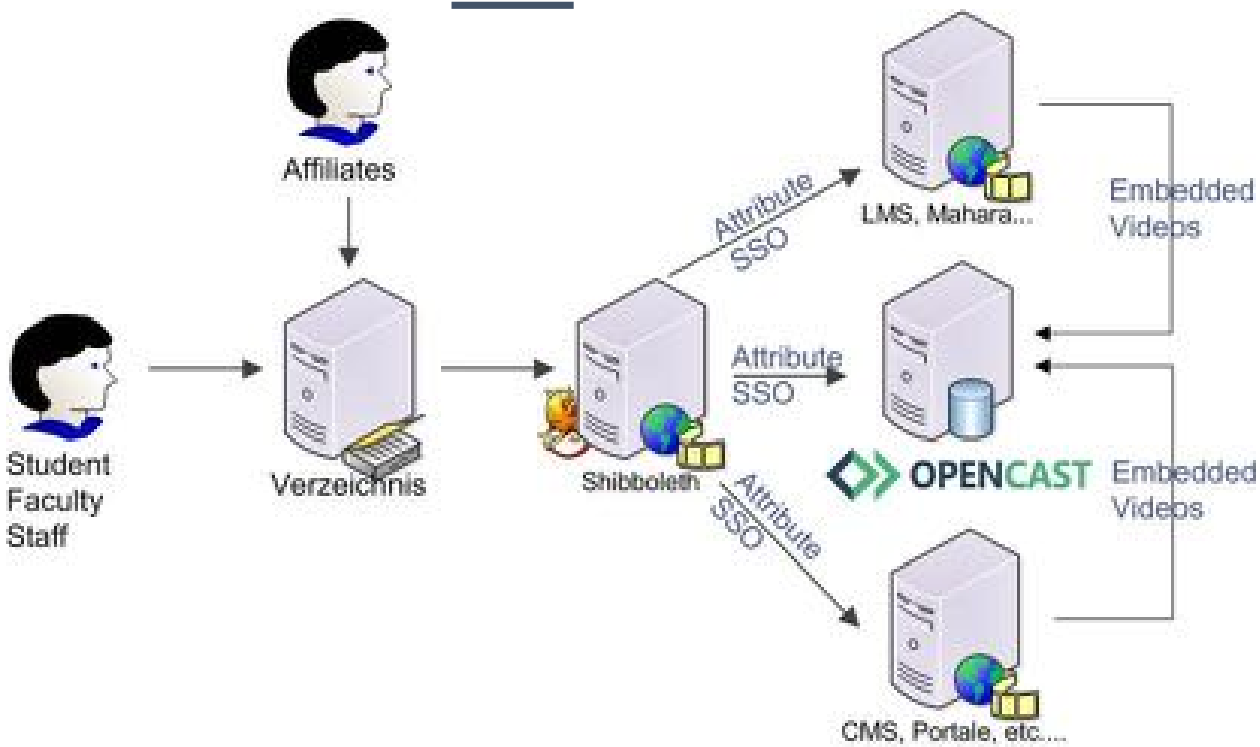


Embedding Code

Autorisierung im SSO- oder LTI-Kontext

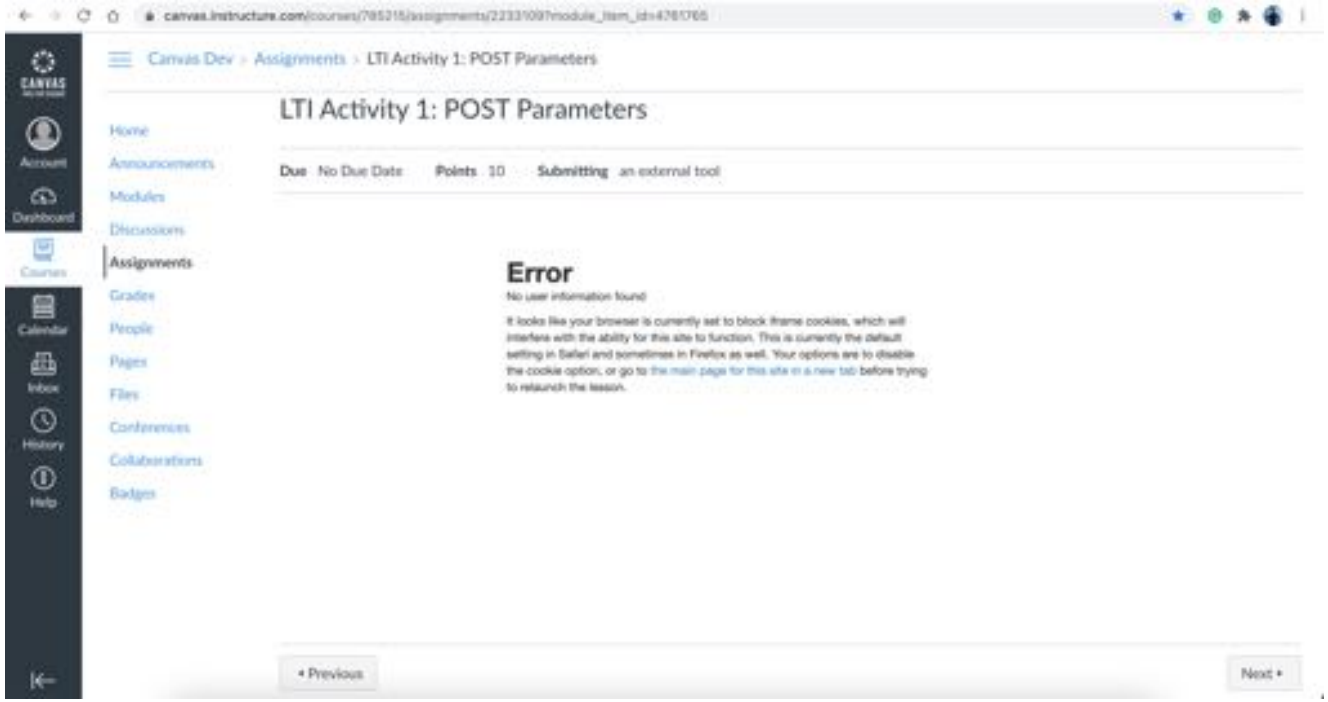
Background Autorisierung

Embedding Codes in Iframes funktionieren nicht mehr, weder mit LTI noch SSO



LTI 1.2: oauth

LTI Aktivitäten in LMSen können in Iframes keine Nutzerdaten mehr übermitteln



LTI Tools

Nicht mehr im Iframe verwenden

Im Iframe

Aktuell geht noch SameSite=None

Nach Phase Out von 3rd Party Cookies, ggf. mit CNAMEs arbeiten?

Upgrade auf LTI 1.3 (OIDC), in Moodle seit Version 3.7

In neuem Tab

- ✓ SameSite=Lax
- ✓ Nach Phase Out von 3rd Party Cookies weiterhin funktional

SameSite auf IDPs

Why Do Nothing

...the IdP is functional "enough" such that the advisable course of action for most deployers is to do nothing at present, unless

- ... they use the SAML proxying feature (in unseren Tests nicht nachweisbar)
- ... A SAML 2.0 SP uses the HTTP-POST binding to issue its request (e.g. EZProxy) AND the IdP is configured to use server-side sessions OR is not using HTML Local Storage with client-side sessions (kein SSO)

SAML Proxies sollen ggf. nicht mehr funktionieren (?)

idp.cookie.sameSite and idp.cookie.sameSiteCondition

HTML Local Storage aktivieren

vgl. https://shibboleth.atlassian.net/wiki/spaces/IDP4/pages/1284276231/SameSite

IDP Settings I

Doing Something

Workarounds bis Phase out von 3rd Party Cookies

The filter is pre-installed by default now, but upgraded systems with web.xml modifications would need to import those additions from the delivered version. Even when present, it is disabled by default.

idp.cookie.sameSite and **idp.cookie.sameSiteCondition**, control the operation of the filter. The former sets the default SameSite value to apply to all cookies,...

vgl. https://shibboleth.atlassian.net/wiki/spaces/IDP4/pages/1284276231/SameSite

IDP Settings II

HTML Storage Service – bei geupgradeten Systemen deaktiviert

Empfehlung seit IDP Version 4.0:

idp.properties:

```
idp.storage.htmlLocalStorage = true
```

session-manager.xml:

```
<util:list id="shibboleth.ClientStorageServices">
    <ref bean="shibboleth.ClientSessionStorageService" />
    <ref bean="shibboleth.ClientPersistentStorageService" />
</util:list>
```

vgl. https://shibboleth.atlassian.net/wiki/spaces/DEV/pages/1181253974/IdP+SameSite+Testing

Single Logout

Parallele Logouts in Iframes

HM

Möchten Sie sich von allen Diensten abmelden, auf die Sie während Ihrer Webbrowser Sitzung zugegriffen haben?

Ja, alle Dienste

Nein

Wenn Sie auf **Ja** klicken, wird das System sie auch von den folgenden Diensten abmelden:

1. Moodle Instanz für vhb bei ssystems
2. Moodle-Lernplattform der Hochschule München

Impressum Hilfe / FAQ Dunkles Design

Paralleler SLO in Iframes

Redirects (Top Level Navigation) unzuverlässig

HM

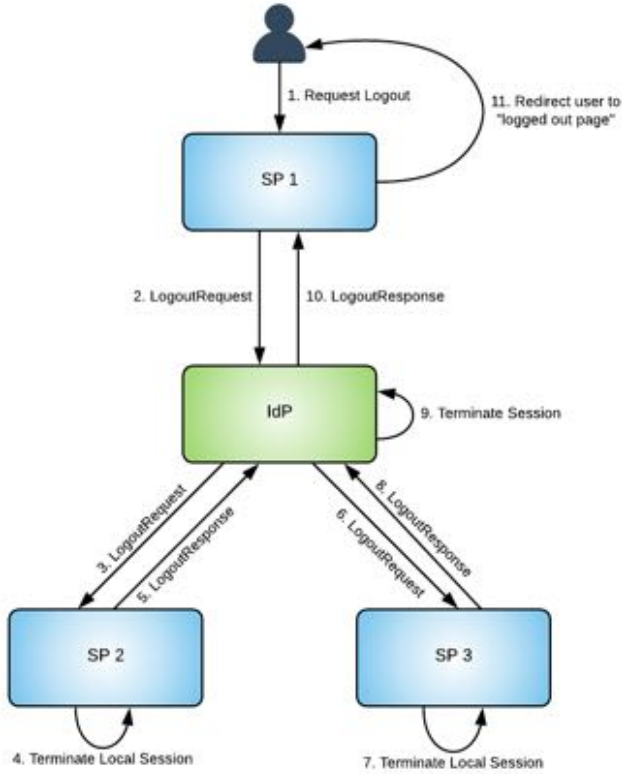
Versuch gestartet um Sie bei folgenden Diensten abzumelden:

1. Moodle-Lernplattform der Hochschule München
2. Moodle Instanz für vhb bei ssystems

Impressum Hilfe / FAQ Dunkles Design

Paralleler SLO in Iframes

PropagateLogout Flow



Quelle: https://www.identityserver.com/articles/the-challenge-of-building-saml-single-logout

Single Logout (SLO) I

Bindings – Metadata anpassen

Relevante SLO Bindings (SingleLogoutServices):

- *urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact*
- urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST
- urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect
- urn:oasis:names:tc:SAML:2.0:bindings:SOAP
- Message Correlation (inResponseTo) spielt keine Rolle

Erster Endpoint in Metadata zählt

Oft Artifact der erste, ausgehend Port 8443 notwendig

Reihenfolge in mdv.aai.dfn.de nicht (mehr) möglich?

vgl. https://shibboleth.atlassian.net/wiki/spaces/SP3/pages/2093318581/SameSite
grep -2 SLO/Artifact dfn-sp-metadata.xml

Single Logout (SLO) II

Das erste in den Metadata wird genommen – aufraeumen!

SLO is unaffected for either HTTP-Redirect or HTTP-POST bindings:

- *Bei SLO request zu einem Shibboleth SP sind session cookies optional*
- Artifact und SOAP sind Backchannel, keine cookies involviert
- Message Correlation bei IDP initiated Logout nicht relevant

Session Cookie wird geblockt

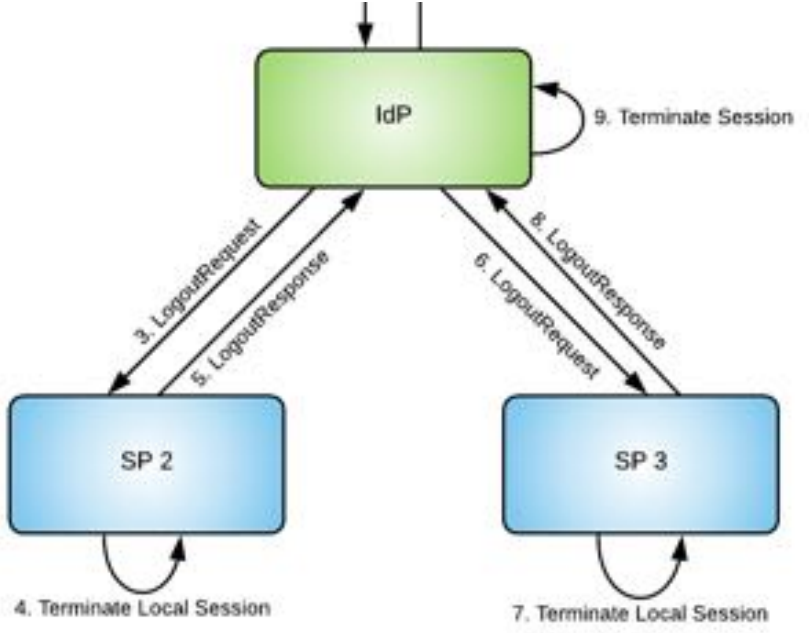
NameID in Assertion ausreichend

Application Cookie wird geblockt (notify)!

vgl. https://shibboleth.atlassian.net/wiki/spaces/DEV/pages/1181253974/IdP+SameSite+Testing

SLO Notify in Iframes

Beendigung von Application Sessions



Quelle: https://www.identityserver.com/articles/the-challenge-of-building-saml-single-logout

Notify Elements

Application Session Logout

Front Channel Logout: SameSite=none:

Application Cookie benötigt SameSite=none (!)

Nach Phase Out von 3rd Party Cookies nicht mehr möglich

```
<Notify Channel="front"
Location="https://moodle.ssystems.de/auth/shibboleth/logout.php"/>
```

Back Channel Logout: keine Cookies beteiligt

- ✓ Shibboleth Session und Application Session verknüpfen
- ✓ Frank Schreiterer (Uni Bamberg):

  https://doku.tid.dfn.de/de:shibslohttpd:introduction

```
<Notify Channel="back"
Location="https://moodle.ssystems.de/auth/shibboleth/logout.php"/>
```

Beispiel Moodle

Front Channel und Back Channel Logout

Front Channel Logout

```
if (isloggedin($USER) && $USER->auth == 'shibboleth') {
    // Logout user from application.
    require_logout();
}
```

Back Channel Logout (SOAP Handler!):

```
function LogoutNotification($spsessionid) {
    ...
    helper::logout_db_session($spsessionid);
}
```

vgl. https://github.com/moodle/moodle/blob/master/auth/shibboleth/logout.php

First Party Sets

Deklarativ Origins vereinen

Integration von FPS: /.well-known/first-party-set

```
// https://a.example/.well-known/first-party-set
{
  "owner": "a.example",
  "members": ["b.example", "c.example"],
}
// https://b.example/.well-known/first-party-set
{
        "owner": "a.example"
}
// https://c.example/.well-known/first-party-set
{
        "owner": "a.example"
}
```

First Party Sets II

Kritik von W3C Technical Architecture Group (TAG)

Eigenschaften von FPS:

In short, First-Party Sets would shift Web privacy from something users can control to something websites control."

- Man kann nur einem First Party Set angehören, nicht transitiv
- Set-Cookie: session=123; Secure; SameSite=Lax; SameParty
- https://github.com/WICG/first-party-sets#clearing-site-data-on-set-transitions

Aufweichung von Same-Site

Nicht in AAI geeignet

Missbrauch durch Rewrite Rules ?

vgl. https://brave.com/web-standards-at-brave/8-first-party-sets/

Hands On

Roadmap in a nutshell

IDP: idp.storage.htmlLocalStorage = true
SP: sameSiteFallback=true

Konfigurationen aktualisieren

SameSite=None hilft nicht mehr

2024 Phase Out von 3rd Party Cookies

SameSite Settings

SameSite=None hilft noch

Front Channel notify auf Back Channel umstellen

Anpassung von Anwendungen notwendig

FedCM und FPS

Ggf. 3rd Party Cookies im AAI Kontext wieder möglich

ssystems Consulting

Ihr Partner für innovative Digitalisierung

info@ssystems.de

030202360710

www.ssystems.de