



online studieren

Einfluss neuer Cookie-Richtlinien auf SSO und SLO

systems 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,...



E-Learning, E-Prüfung

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



Server und Infrastruktur

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

Hosted in
Germany



Anwendungsentwicklung

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

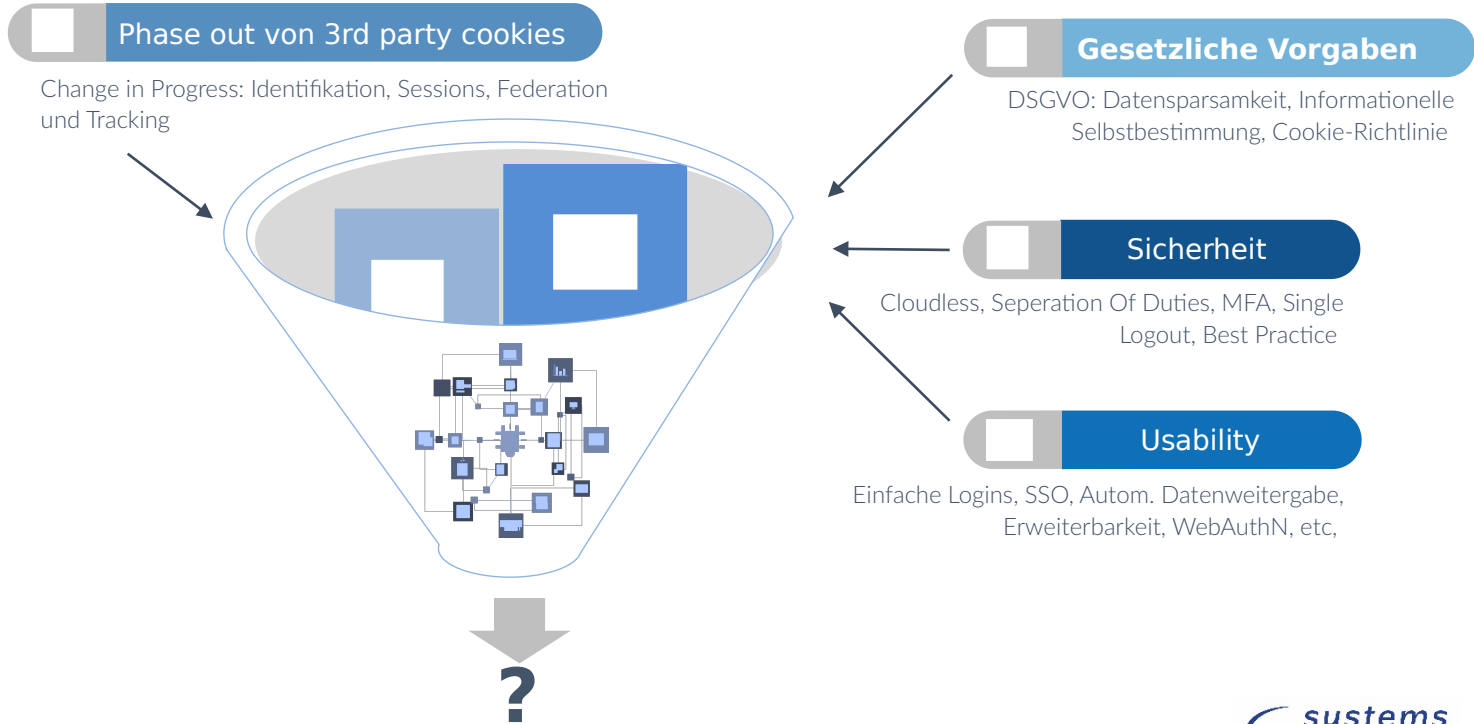
Einige Referenzen

Nachhaltige Dienstleistungen



Motivation

Das Spannungsfeld zwischen Usability, Security und Compliance

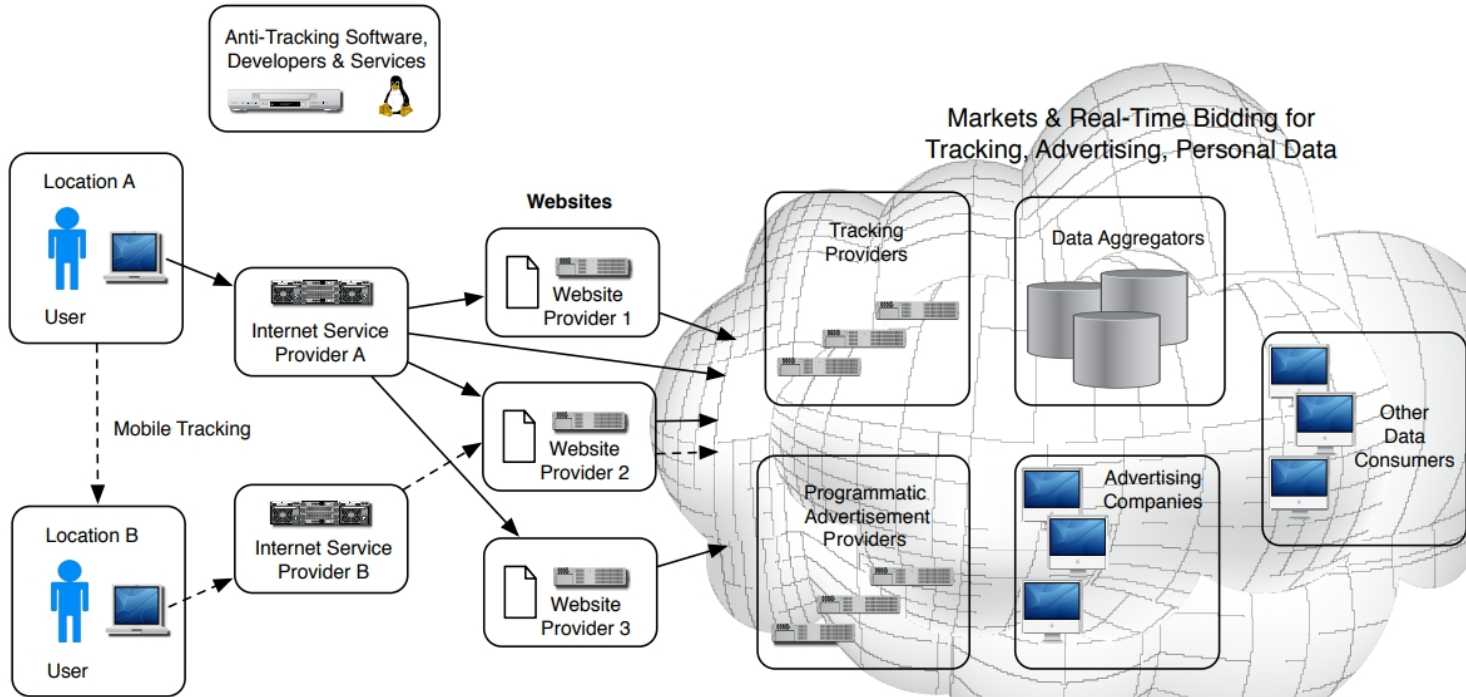


Web Tracking

PRIVACY

TECHNOLOGY

COMMERCIAL



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

1st Party Data



User browses to website A



Website plants a 1st party cookie to identify them when they return.

3rd Party Data



User browses to website A



Website plants a 3rd party cookie (like an ad network).



When the user visits website B for the first time, they are already identified by the network and served targeted ads.



The network collects the user info (for examples, which sites and pages they have visited) and allows advertisers to target that user when they visit another site.

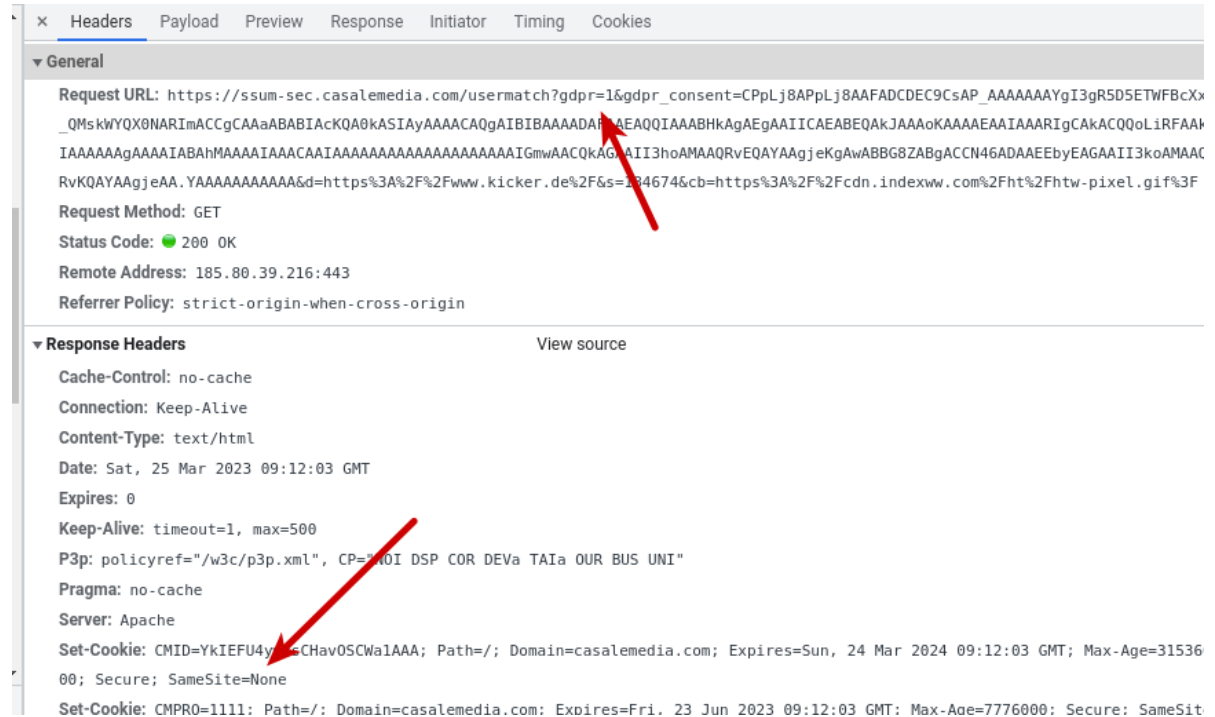
Quelle: <https://www.singlegrain.com/advertising/privacy-sandbox/>

ssystems GmbH | Berlin | 28.03.2023 | Harald Strack



EU Cookie-Richtlinie

IFRAME, IMG, JS, ...



Headers Payload Preview Response Initiator Timing Cookies

General

Request URL: https://ssum-sec.casalemedia.com/usermatch?gdpr=1&gdpr_consent=CpPlj8APpLj8AAFADCEC9CsAP_AAAAAAYgI3gR5D5ETWFBcXx_QMskwYQX0NARImACcgCAAaABABIAcKQa0kASIAyAAAAQgAIBIBAAAAADAI_AEAQIaABHkAgAEgAAIICAEBEQakJAAAoKAAAAEAAIAARIGcAkACQoLiRFAAIIAAAAAgAAAAIABAhMAAAAIAAACAAIAAAAAAAAAAAAAAAAAAAAGmwAACQkAG_AII3hoAMAAQrVeqYAAgjeKgAwABBG8ZABgACCN46ADAAEEbyEAGAAII3koAMAAARvKQAYAAgjeAA.YAAAAAAAAAAAA&d=https%3A%2F%2Fwww.kicker.de%2F&s=134674&cb=https%3A%2F%2Fcdn.indexww.com%2Fht%2Fhtw-pixel.gif%3F

Request Method: GET

Status Code: 200 OK

Remote Address: 185.80.39.216:443

Referrer Policy: strict-origin-when-cross-origin

Response Headers [View source](#)

Cache-Control: no-cache

Connection: Keep-Alive

Content-Type: text/html

Date: Sat, 25 Mar 2023 09:12:03 GMT

Expires: 0

Keep-Alive: timeout=1, max=500

P3p: policyref="/w3c/p3p.xml", CP="NOI DSP COR DEVa TAIa OUR BUS UNI"

Pragma: no-cache

Server: Apache

Set-Cookie: CMID=YkIEFU4y...sCHav0SCWaIAAA; Path=/; Domain=casalemedia.com; Expires=Sun, 24 Mar 2024 09:12:03 GMT; Max-Age=3153600; Secure; SameSite=None

Set-Cookie: CMPRO=1111; Path=/; Domain=casalemedia.com; Expires=Fri, 23 Jun 2023 09:12:03 GMT; Max-Age=7776000; Secure; SameSite=None

studieren

shift

Quantitative Betrachtung

Anteil der Tracking- und AD-Requests > Inhalte

Chrome Browser

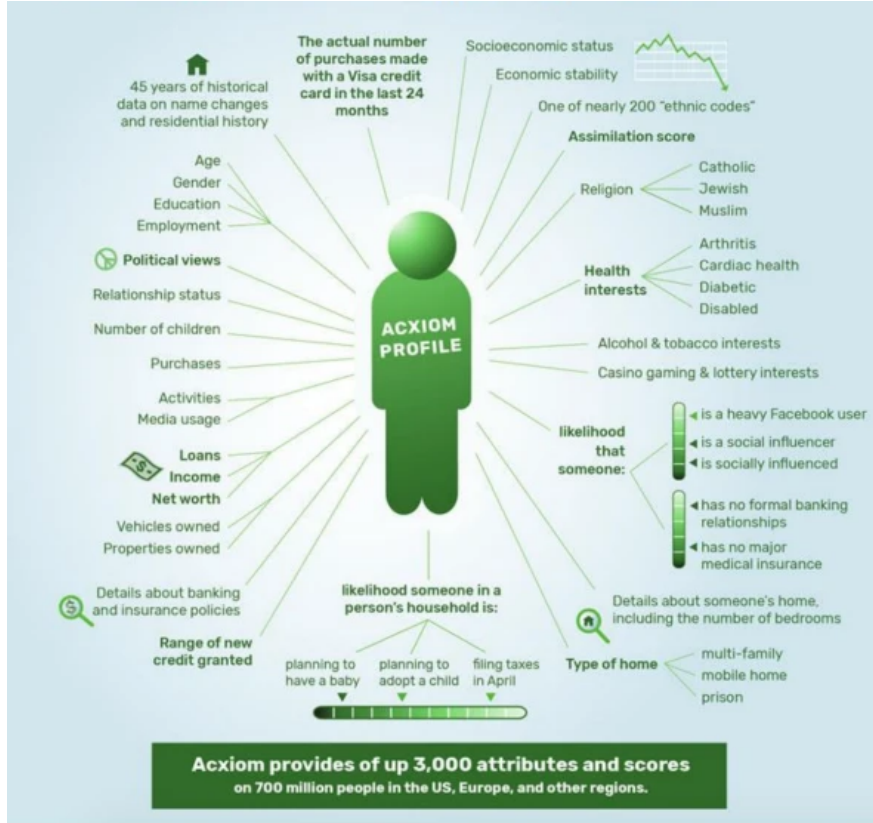


Brave Browser



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...



Dr. Paul Vixie

Oportunistic abuse of internet protocols

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

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>

ssysteme GmbH | Berlin | 28.03.2023 | Harald Strack

Exkurse

Cookies und Googl Privacy Sandbox

Florian Ritterhoff

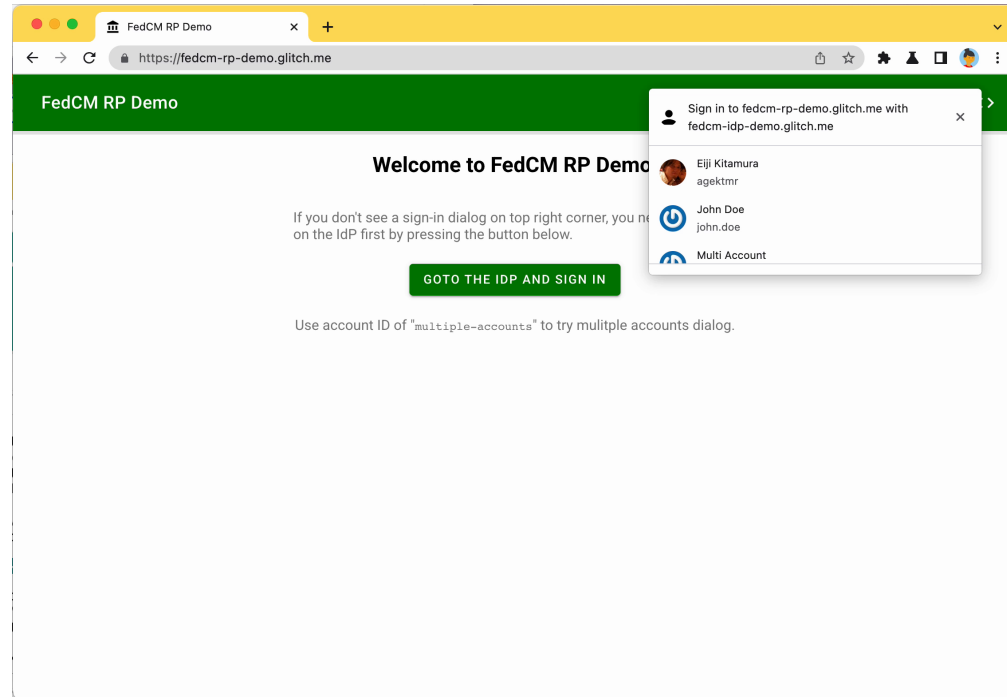
Deep Dive in technische Aspekte von Cookies

Michael Fuchs

Google Privacy Sandbox

FedCM

Federated Credential Management API



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

ssystems GmbH | Berlin | 28.03.2023 | Harald Strack



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>

ssystems GmbH | Berlin | 28.03.2023 | Harald Strack

Embedding von Videos

Autorisierung bei aktivem Top Level SSO Kontext

The screenshot displays a web application interface. At the top, a navigation bar includes links for Home, Dashboard, Events, Meine Kurse, Dieser Kurs, Hilfe, and Kurse. Below this, a breadcrumb trail shows 'Kurse'. A left-hand sidebar contains a settings menu under the heading 'Einstellungen'. The menu items are: Textseite-Administration (with sub-items: Einstellungen, Lokale Rollen zuweisen, Rechte ändern, Rechte prüfen, Filter, Logdaten, Sicherung, Wiederherstellen), Kurs-Administration, and Website-Administration. A search bar with a 'Suchen' button is located at the bottom of the sidebar. The main content area shows a video player with a play button overlay. The video title is 'Technische Mechanik: Beispiel 4.1 - Berechnung der L... Einzelast'. Below the video player, the text 'Zuletzt geändert: Saturday, 22. December' is visible.

Embedding Code

Autorisierung im SSO- oder LTI-Kontext

Embedding code

620x349

540x304

460x259

380x214

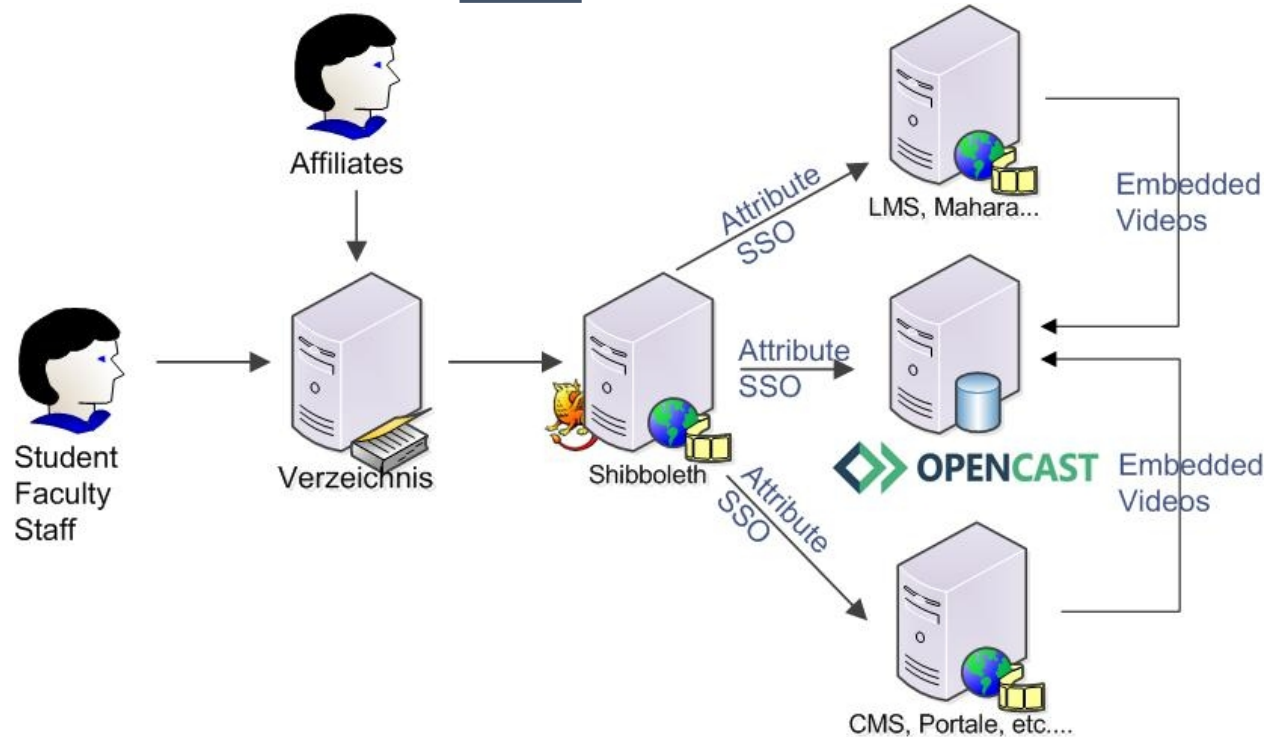
300x169

```
<iframe allowfullscreen src="<SERVER_URL>/paella/ui/watch.html?id=5af27df7-dd43-4fcc-b005-e4ba935c6ca9" style="border:0px #FFFFFF none;" name="Paella Player" scrolling="no" frameborder="0" marginheight="0px" marginwidth="0px" width="460" height="259"></iframe>
```

Copy to clipboard

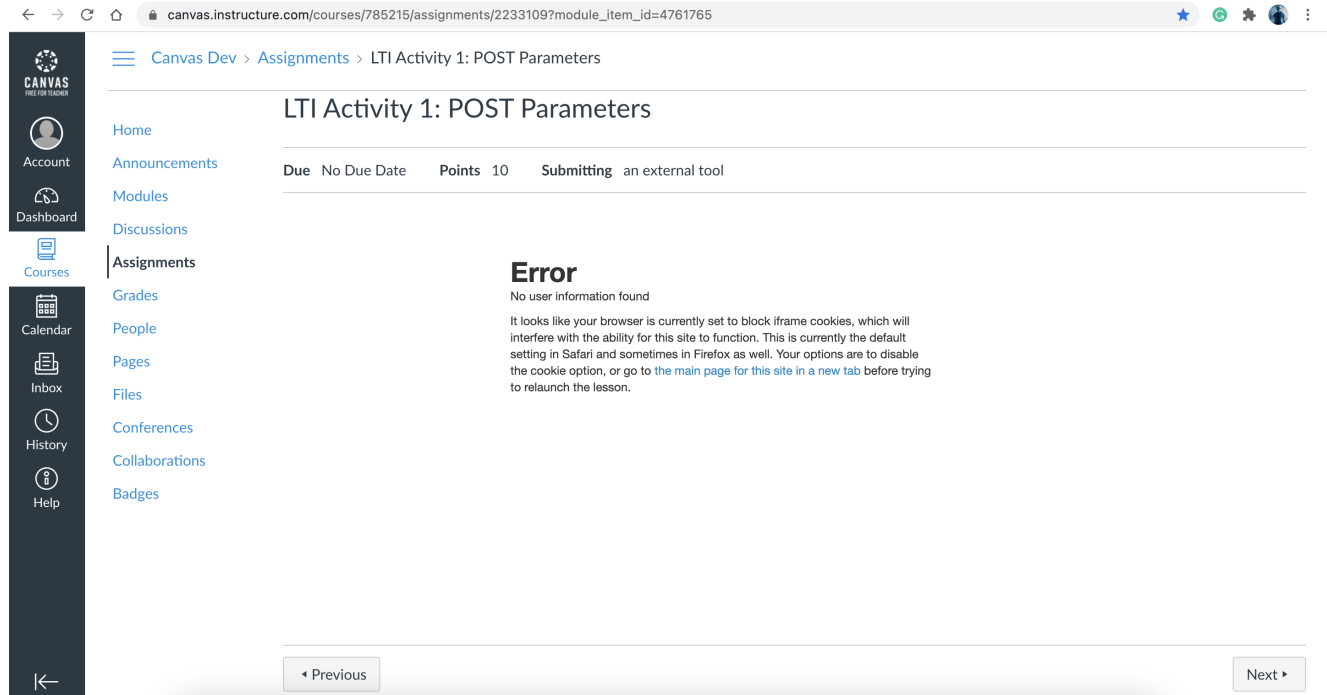
Background Autorisierung

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



The screenshot shows a web browser window with the URL `canvas.instructure.com/courses/785215/assignments/2233109?module_item_id=4761765`. The page title is "LTI Activity 1: POST Parameters". The left sidebar contains navigation links: Home, Announcements, Modules, Discussions, Assignments (selected), Grades, People, Pages, Files, Conferences, Collaborations, and Badges. The main content area displays an error message:

Error
No user information found

It looks like your browser is currently set to block frame cookies, which will interfere with the ability for this site to function. This is currently the default setting in Safari and sometimes in Firefox as well. Your options are to disable the cookie option, or go to [the main page for this site in a new tab](#) before trying to relaunch the lesson.

Navigation buttons at the bottom include "◀ Previous" and "Next ▶".

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>

ssystems GmbH | Berlin | 28.03.2023 | Harald Strack

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>

ssystems GmbH | Berlin | 28.03.2023 | Harald Strack



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>

ssystems GmbH | Berlin | 28.03.2023 | Harald Strack

Single Logout

Parallele Logouts in Iframes



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



Versuch gestartet um Sie bei folgenden Diensten abzumelden:

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

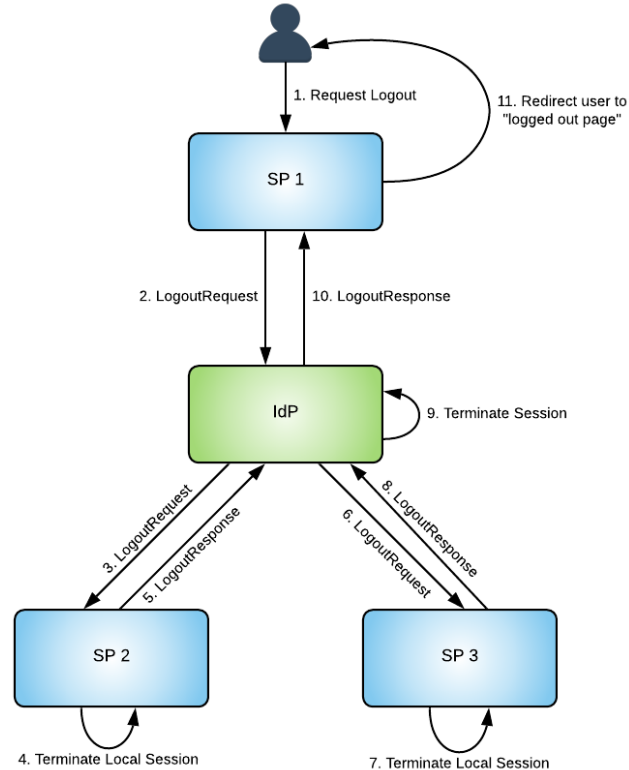
[Impressum](#)

[Hilfe / FAQ](#)

Dunkles Design

Paralleler SLO in Iframes

PropagateLogout Flow



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 – aufräumen!

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

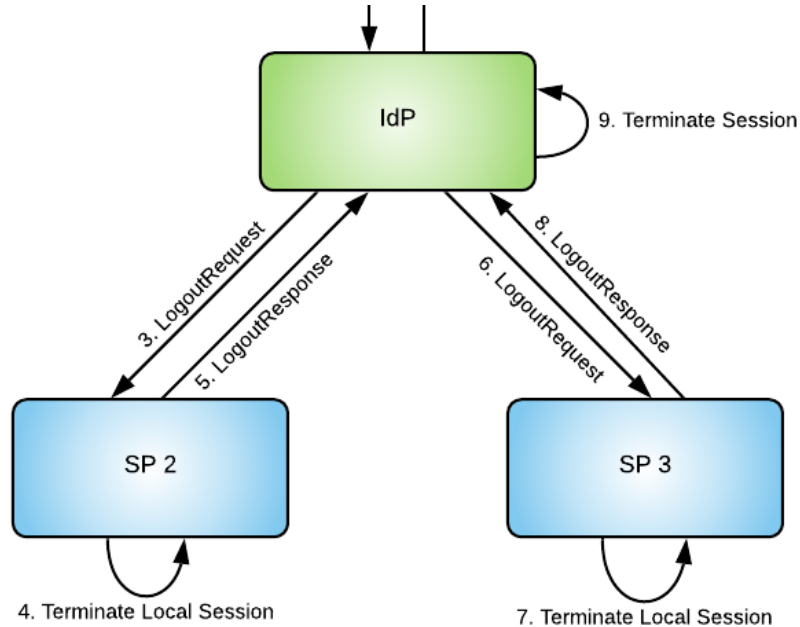
➔ Session Cookie wird geblockt

➔ NameID in Assertion ausreichend

➔ Application Cookie wird geblockt (notify)!

SLO Notify in Iframes

Beendigung von Application Sessions



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>

ssystems GmbH | Berlin | 28.03.2023 | Harald Strack

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>

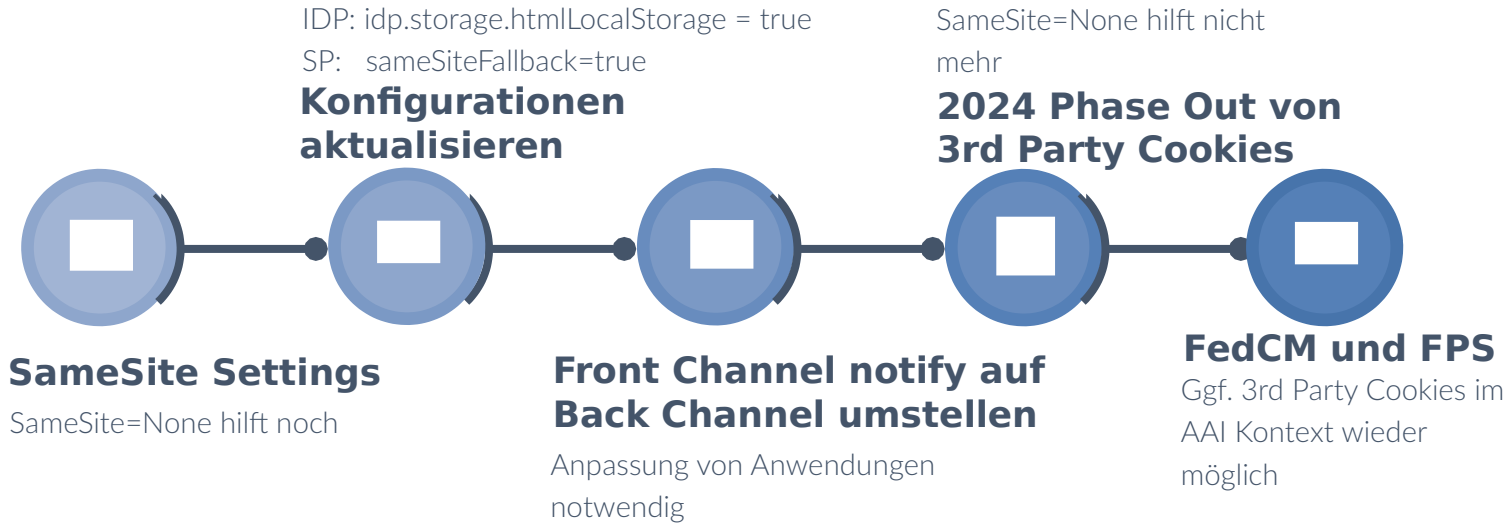
➔ **Aufweichung von Same-Site**

➔ **Nicht in AAI geeignet**

➔ **Missbrauch durch Rewrite Rules ?**

Hands On

Roadmap in a nutshell




ssystems Consulting

Ihr Partner für innovative Digitalisierung

online studieren

 info@ssystems.de

 030202360710

 www.ssystems.de