Logout-Propagation mit Shibboleth IdP in Proxy-Szenarien

80. DFN Betriebstagung / Forum AAI
Berlin, 19.03.2024

Peter Gietz, David Hübner
DAASI International GmbH

Agenda

- Einführung in SLO
- SLO und Third Party Cookies (FedCM)
- SLO und Proxies
- Propagation Plugin

DAASI International

Warum Singe Log-Out

- Bei SAML Single Sign-On werden nach einer einmaligen Authentifizierung, beliebig viele authentifizierte Sessions mit Anwendungen aufgebaut.
- Ohne SLO bleiben alle diese authentifizierten Sessions vorerst erhalten
- Offene nicht mehr genutzte Sessions sind grundsätzlich ein Sicherheitsproblem, da sie gehijacket werden können
- Insbesondere, wenn ein Rechner von mehreren Nutzern genutzt werden, können spätere User die Sessions eines früheren Users nach nutzen, also sich als Letzteren ausgeben und dessen Rechte nachnutzen
- Da SLO aber recht komplex ist (s.u.) wird es seltener genutzt

DAASI International

Drei Arten von SAML Logout

- Beim Shibboleth IdP für SAML2: Unterscheidung in

  1) Local Logout am SP (der IdP ist gar nicht involviert)
  2) Simple/Proprietary Logout (Shibboleth IDP-spezifisch) /idp/profile/Logout
  3) SAML Logout (über SAML-Protokoll-Nachrichten <LogoutRequest>)

- Zusätzlich bei (2) und (3) die Option für „Logout Propagation“ (=SLO mit weiteren an der Session beteiligten SPs)
- Der einzig standardisierte Weg ist (3)* und sollte daher bevorzugt werden

* vgl. „Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, Kap. 4.4, https://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

DAASI International

Logout Propagation / SLO

- Es werden alle SPs benachrichtigt, die eine aktive Session am IdP haben
- Der IdP muss SP-Sessions tracken (inzwischen Standard-Einstellung)
- User wird dann beim Logout am IdP (Simple oder SAML) gefragt, ob Propagation gewünscht
- Propagation kontaktiert (siehe nächste Slide) die Logout-Endpunkte aller SPs, die im Rahmen der gerade beendeten SSO-Session eine aktive Session haben
- <LogoutRequest> an jeden SP...
- ... jeder SP antwortet mit <LogoutResponse>, IdP stellt Ergebnis grafisch dar
- Der Browser *bleibt* dabei auf der Logout-Seite des IdP!

DAASI International

Backchannel vs. Frontchannel Logout

- Für die technische Umsetzung des <LogoutRequest> bei der SLO-Propagation gibt es zwei Möglichkeiten:
  1) Bei Frontchannel-Logout wird der Aufruf des Logout-Endpunkts des SPs im Browser (Frontchannel) dargestellt. Dafür kommt ein (verstecktes) I-Frame bzw. Bild zum Einsatz. Die Session kann am SP über den Session-Cookie gemappt werden. **(*)**
  2) Beim Backchannel-Logout kontaktiert der IdP den Logout-Endpunkt des SPs serverseitig. Die Session am SP muss ebenfalls serverseitig vorliegen.
- **(*)** Aus Browser-Sicht handelt es sich dabei um Third-Party-Cookies. Es gibt Bestrebungen, diese in den Browsern standardmäßig zu verbieten, da diese das Standardmittel zu User-Tracking für Werbezwecke sind.
- Damit wird Frontchannel-Logout unmöglich. Backchannel ist davon nicht betroffen, wird aber weniger häufig von SPs unterstützt.
  - Für Forschungsinfrastrukturen in denen die SPs meist unter ähnlicher Kontrolle sind, wäre eine Backchannel-Lösung denkbar
- Eine mögliche Alternative sind Entwicklungen wie FedCM.

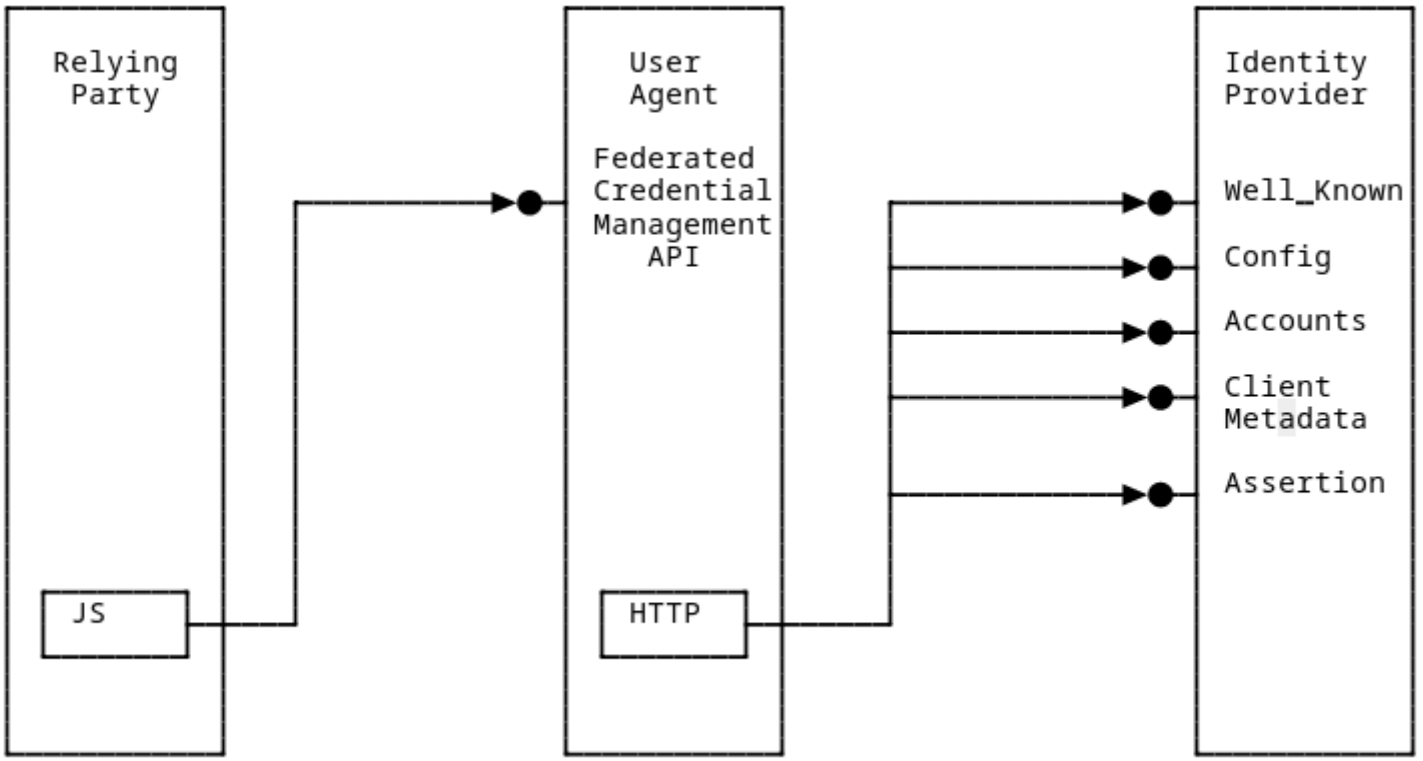
DAASI International

FedCM

- Federated Credential Management API:
  - „a standard mechanism for identity providers (IdPs) to make identity federation services available on the web in a privacy-preserving way, without the need for third-party cookies and redirects“*
  - Dieses Ziel wird erreicht durch die Einführung eines Useragent im Browser, der entsprechende API-Aufrufe macht
  - Die Entwicklung ist insbesondere getrieben durch Google und Mozilla
  - Im Rahmen einer W3C Community Group wurde ein erster Draft verabschiedet.
  - Im Augenblick wird an der Gründung einer W3C Working Group gearbeitet, um daraus einen W3C-Standard machen zu können

Vgl. https://developer.mozilla.org/en-US/docs/Web/API/FedCM_API

FedCM



Vgl. Federated Credential Management API Draft Community Group Report, 28 February 2024
https://fedidcg.github.io/FedCM/#browser-api-identity-credential-interface

Logout in OIDC

- Auch in OIDC gibt es Profile für SLO
- Auch hier wird zwischen Frontchannel und Backchannel unterschieden*
- Auch hier gibt es bei Frontchannel die Abhängigkeit von 3rd Party Cookies
- Auch hier ist FedCM eine mögliche Lösung auch dieses Problems
- Beim Einsatz des Shibboleth OIDC OP-Plugins wird derzeit nur „Simple/Proprietary Logout“ unterstützt, wobei eine breitere Unterstützung der OIDC-Logout-Flows in Arbeit ist

* vgl. M. Jones: OpenID Connect Front-Channel Logout 1.0, https://openid.net/specs/openid-connect-frontchannel-1_0.html bzw.
M. Jones: OpenID Connect Back-Channel Logout 1.0 , https://openid.net/specs/openid-connect-backchannel-1_0.html

DAASI International

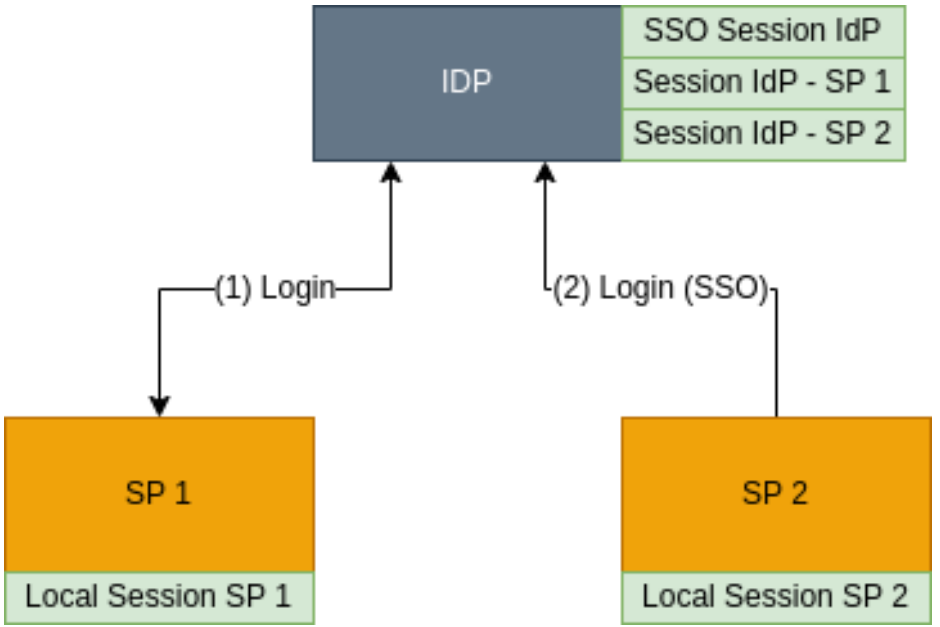
Proxy-Funktionalität im Shibboleth IdP

- Seit AARC wissen wir: (fast) jedes Problem ist mit einem Proxy zu lösen
- Inzwischen unterstützt der Shibboleth IdP Proxy-Funktionalität für SAML (authn/SAML) und OIDC (authn/OIDCRelyingParty)
- Dabei wird die Authentifizierung an einen externen IdP delegiert
  - Beispiel 1: Weiterreichen des Login an ein existierendes SSO-System (Shibboleth IdP nur für Föderations-Dienste oder zur Unterstützung von OIDC)
  - Beispiel 2: Shibboleth IdP als Proxy zur Föderation, welcher zusätzliche Attribute beisteuert (Usecase Edu-ID oder NFDI)
- Standardmäßig endet am Proxy der Logout-Prozess. Der Proxy kümmert sich bei SLO nur um die eigene Session und die direkt verbundenen SPs.

DAASI International

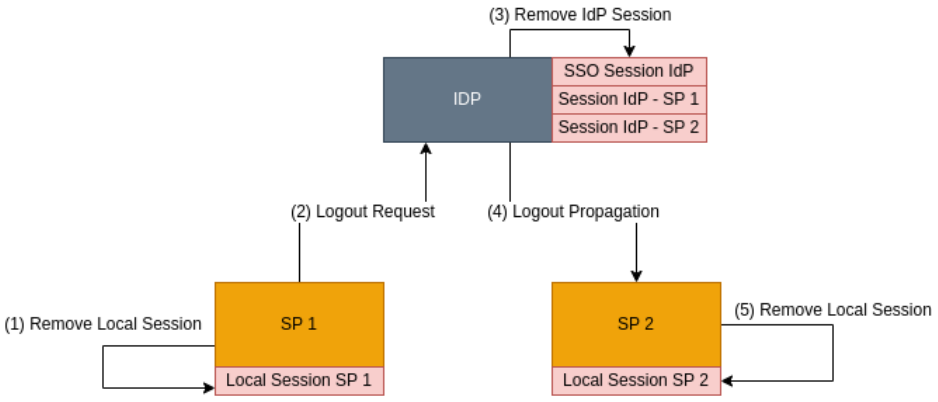
SLO ohne Proxy

- Ausgangsszenario
  - Login bei zwei SPs (SP 1 und SP 2)
  - Beide SPs haben eine lokale Session
  - Der IdP hat eine SSO-Session
  - Der IdP weiß, dass im Rahmen der SSO-Session Zugriff auf SP 1 und SP 2 erfolgt ist



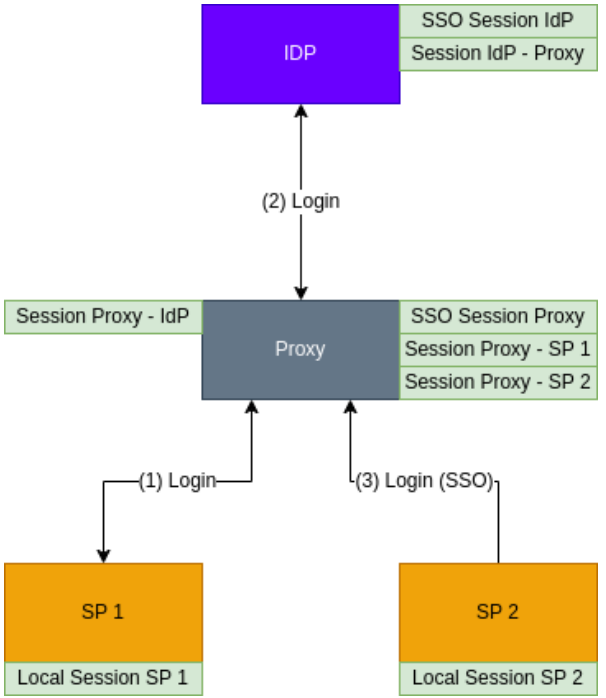
SLO ohne Proxy

- In SP 1 wird ein Logout ausgelöst
- SP 1, SP 2 und IdP beherrschen Single Logout
- SP 1 beendet lokale Session und schickt Logout Request an IdP (Schritte 1 und 2)
- IdP beendet SSO-Session und propagiert Logout Request an SP 2 (Schritte 3 und 4)
- SP 2 beendet lokale Session (Schritt 5)
- Ergebnis: Alle Sessions sind beendet



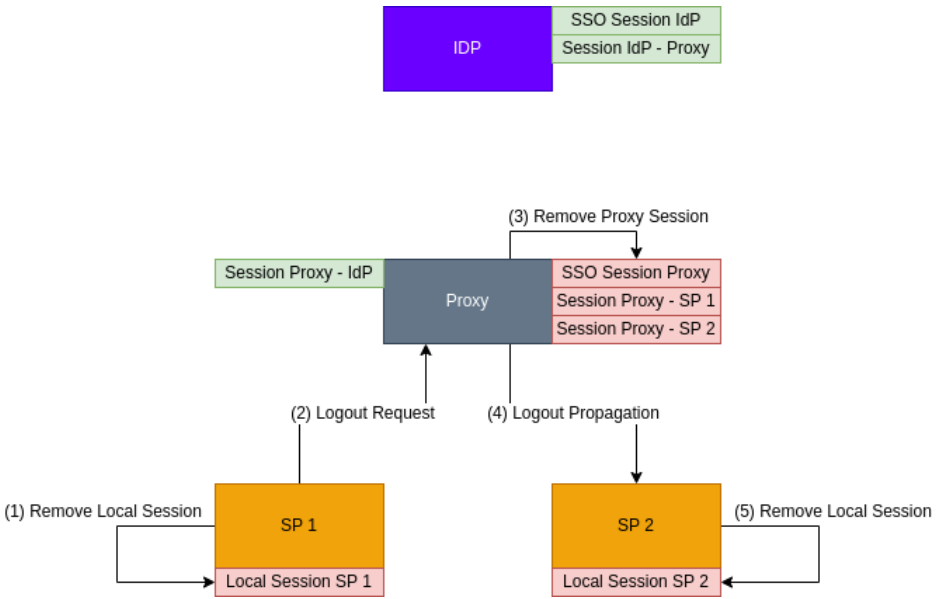
SLO mit Proxy

- Ausgangsszenario:
  - Der Proxy leitet den Login an einen weiteren IdP weiter. Dabei tritt der Proxy gegenüber dem IdP als SP auf (Schritt 2)
  - Neben den aus dem „ohne Proxy“-Fall bekannten Session existiert:
    - Session zwischen Proxy und IdP
    - SSO-Session am IdP



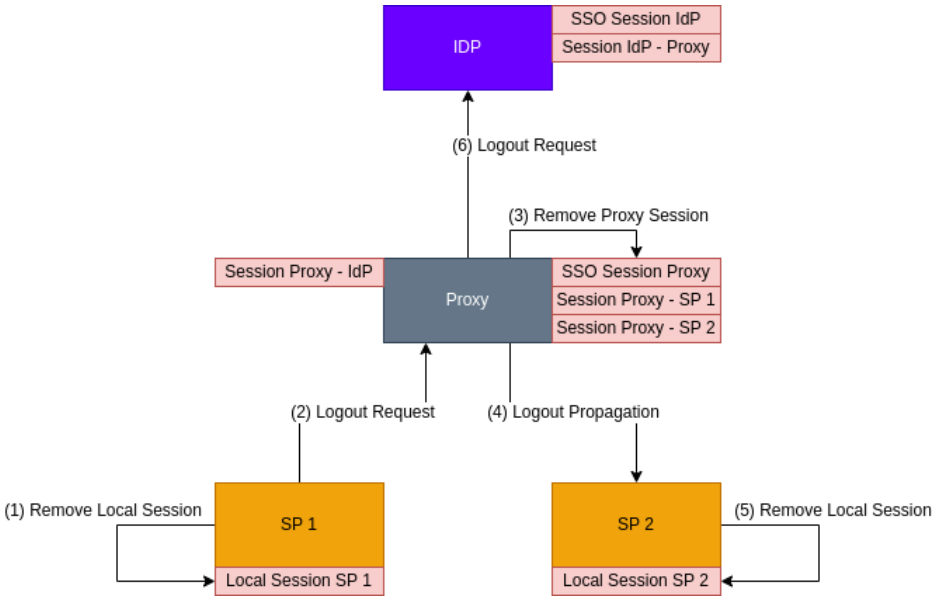
SLO mit Proxy

- Teil 1 von SLO (Schritte 1 bis 5) wie im Fall ohne Proxy
- Probleme
  - IdP hat weiterhin eine Session. Bei einem erneuten Login SP 1 → Proxy → IdP werden alle Sessions ohne Interaktion wieder erzeugt.
  - Etwaige Sessions zwischen IdP und anderen SPs sind unberührt



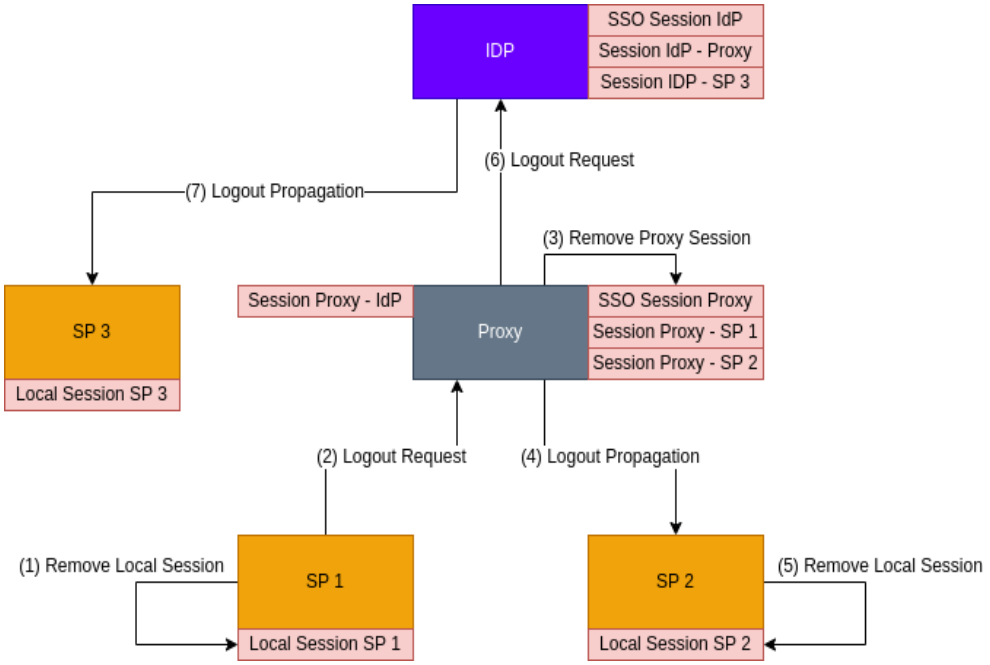
SLO mit Proxy und Logout-Propagation

- Lösung:
  Proxy-Logout-Propagation als Shibboleth-IdP-Plugin am Proxy
- Teil 2 von SLO (Schritt 6) nutzt die gespeicherte „Proxy – IdP“-Session für einen Logout-Request an den IdP
- Ergebnis: IdP kann SSO-Session ebenfalls beenden ...

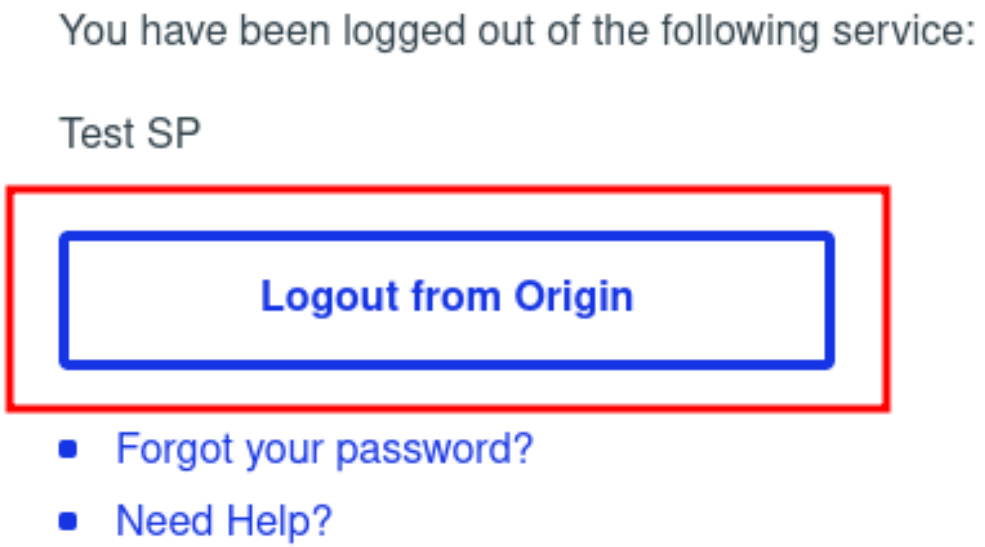


SLO mit Proxy

- ... und etwaige weitere SPs, welche nur bei IdP eine Session haben, über eine weitere Logout-Propagation (Schritt 7) benachrichtigen



Angepasster Logout-Screen am Proxy-IdP



Proxy-Propagation-Plugin

- Das Proxy-Logout-Propagation-Plugin wurde von DAASI International ursprünglich für das Alfred-Wegener-Institut (AWI) entwickelt
- Mit dem erklärten Ziel, dass der Code open-source wird und möglichst als offizielles Plugin langfristig vom Shibboleth-Consortium gepflegt wird
- We will keep you updated

DAASI International

Ausblick

- DAASI International arbeitet in Kooperation mit Google an einem PoC für ein Shibboleth IdP Plugin, das Frontchannel SLO via FedCM ermöglicht
  - Wir hijacken sozusagen die FedCM-API an einer ganz bestimmten Stelle um SAML Frontchannel-Logout funktional zu halten.
- Weitere Privacy enhancing Funktionen im Browser könnten weitere SAML-Flows beeinträchtigen: Verhindern von Tracking:
  - Vgl. Navigational-Tracking Mitigations
    Draft Community Group Report, 28 September 2023
    https://privacycg.github.io/nav-tracking-mitigations/

DAASI International

Vielen Dank für Ihre Aufmerksamkeit!

DAASI International

Tel.: 07071 407109-0

E-Mail: info@daasi.de

Web: www.daasi.de