HTWK Leipzig University of Applied Sciences

Masterarbeit

Solid-basierte erweiterte Zugriffskontrolle und Rückverfolgbarkeit in datengetriebenen webbasierten Systemen

Florian Gudat

Version 43554df, 2024-08-07

Table of Contents

Das Solid-Projekt ist ein RDF-basiertes Ökosystem, das ein dezentralisiertes Web für Einzelpersonen, soziale Einrichtungen oder Software schaffen soll. Die Technologie befindet sich noch in der Entwicklung und ist noch nicht vollständig ausgereift. In dieser Arbeit wird ein experimenteller, herstellerunabhängiger Ansatz zur Erweiterung von Solid über einen serverseitigen Anwendungsschicht-Proxy vorgeschlagen, um die Nachvollziehbarkeit und Zugriffskontrolle angeforderter Ressourcen zu verbessern. Außerdem werden die Auswirkungen dieses Ansatzes auf das Systemdesign und die Leistungseffizienz untersucht.

Kurz & knapp

- Die Masterarbeit beleuchtet den Einsatz eines Datenschutzcockpits als serverseitiger Anwendungsschicht-Proxy im Solid-Ökosystem.
- Starke Einschränkung der Leistungsfähigkeit und des Funktionsumfangs von Solid durch das vorgeschlagene Verfahren.
- Ergebnis: Das Verfahren sollte so nicht eingesetzt werden, auch wenn Zugriffskontrolle und Rückverfolgbarkeit sinnvoll sind.

Das Solid-Projekt beschreibt ein RDF-basiertes Ökosystem, das ein dezentralisiertes Web für Einzelpersonen, Organisationen oder Software schaffen soll. Die Daten werden hierbei sicher in dezentralen Datenspeichern, sogenannten Pods, gespeichert.

Das Ökosystem umfasst eine Reihe von Spezifikationen und zugehörigen Technologien, die hauptsächlich in den technischen Berichten von Solid aufgeführt sind. Die grundlegendste Spezifikation ist das Solid-Protokoll, welches die Identitätsverwaltung und den Mechanismus zur Freigabe von Ressourcen über datengetriebene, webbasierte Schnittstellen regelt. Diese Funktionen werden durch verschiedene Anbieter als Dienstleistung zur Verfügung gestellt und bilden das Fundament für das dezentrale Gesamtsystem.

Chapter 1. Welches Problem lösen Solid-basierte Systeme?

Das Hauptziel des Solid-Projekts besteht in der Umsetzung einer **datensouveränen Identität**. Diese soll die Verfügungsgewalt über die eigenen Daten erhalten und Zugriffskontroll-Mechanismen nutzen können, um selbstständig Zugriffe an weitere Identitäten freizugeben.

Die Verwendung **interoperabler Standards** dient dazu, die Anbieterabhängigkeit zu minimieren. Dadurch wird sichergestellt, dass ein Wechsel des Anbieters ohne Einschränkungen möglich ist. Dies stärkt wiederum die Datensouveränität. In der Regel ist die Verwendung proprietärer Technologien der Grund für die Herausbildung einer hohen Anbieterabhängigkeit. Diese Technologien sind in der Regel nicht mit denen anderer Anbieter kompatibel.

Chapter 2. Herausforderungen in der Zugriffskontrolle und Rückverfolgbarkeit

Das Ökosystem befindet sich derzeit in einem frühen Entwicklungsstadium, weshalb einige Spezifikationen noch im Entwurfsstadium sind. Dadurch können einige Funktionen fehlen, die in produktiven Umgebungen empfohlen werden. Bezüglich der Zugriffskontrolle und Rückverfolgbarkeit ergeben sich folgende Spannungsfelder:

- Das Solid-Protokoll bietet lediglich die Option, den Zugang zu einer Ressource zu genehmigen oder abzulehnen. Eine Nachverfolgung der tatsächlichen Anfrage einer Ressource ist jedoch nicht möglich.
- Das System Solid basiert auf dem Resource Description Framework (RDF) und begünstigt daher den Einsatz vernetzter Daten. Dies bedingt einen erhöhten Bedarf an Rückverfolgbarkeit der Zugriffe auf die Daten.
- Da die Spezifikationen in der Regel einer kontinuierlichen Verbesserung unterliegen oder sich noch in der Entwurfsphase befinden, besteht die Möglichkeit, dass bereits veröffentlichte Versionen Anpassungen unterliegen.
- Das Solid-Ökosystem erfährt eine Erweiterung durch neu eingeführte Spezifikationen bzw. Application Programming Interfaces (APIs).
- Aufgrund der steigenden Nachfrage werden neue Solid-Anbieter eingeführt.

Im Rahmen der Untersuchung wurden die dargestellten Spannungsfelder analysiert. Dabei wurde geprüft, ob ein Solid-basiertes Systemdesign die Transparenz und Zugangskontrolle für angeforderte persönliche Daten verbessern kann. Zudem wurde untersucht, ob das System die Netzwerkschnittstelle herstellerunabhängig nutzen kann, ohne dass es zu einer signifikanten Leistungsminderung kommt.

Chapter 3. Möglichkeiten der Erweiterung der Zugangskontrolle und der Rückverfolgbarkeit im Solid-Ökosystem

Im Rahmen der Untersuchung wurde ein experimenteller Prototyp erzeugt, der als Anwendungsschicht-Proxy zur Beobachtung und Protokollierung für den ein- und ausgehenden Datenverkehr implementiert wurde. Die Anzeige der Protokolldaten erfolgt in Kombination mit einer Web-Anwendung. Beide Komponenten arbeiten mit den im Solid-Protokoll definierten Netzwerkschnittstellen und erweitern das Ökosystem um die Funktionen eines Datenschutzcockpits.

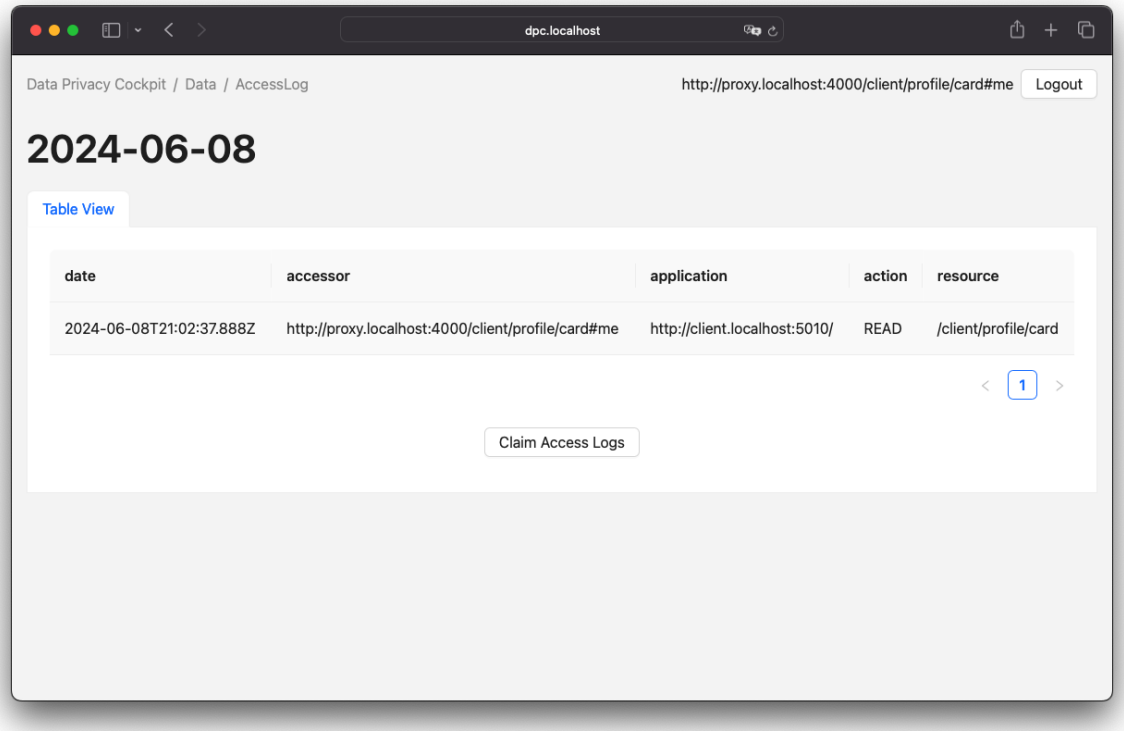

Abbildung 1. Screenshot eines Zugriffsprotokolls in der Webanwendung des Datenschutzcockpits.

Wie in Abbildung 1 dargestellt, wurden das Datum (*date*), die anfragende Identität (*accessor*), der Anwendungskontext (*application*), die Operation auf der Ressource (*action*) und der Pfad der Ressource (*resource*) im Protokoll erfasst. Die Anforderung der Zugriffsprotokolle (*Claim Access Logs*) startet einen anwendungsspezifischen Prozess, der die treuhänderisch gesammelten Zugriffsprotokolle dem Besitzer zur Verfügung stellt.

Chapter 4. Untersuchung zu zukünftigen Anwendungsbereichen des Datenschutzcockpits als Erweiterung des Solid-Ökosystems

Die Untersuchung hat ergeben, dass der für diese Untersuchung erstellte Versuchsprototyp im Betrieb nicht die gewünschte Leistung erbringt. Das beschriebene Verhalten trat bei einzelnen Testläufen mit minimalen Testparametern nicht auf. Bei Erhöhung der Parallelität und der Anzahl der Durchläufe wurden verschiedene Netzwerkfehler beobachtet, die sich durch Anpassung des Experiments bzw. des Versuchsprototyps nicht beheben ließen. Auch eine Variation weiterer Testparameter führte zu einer Abnahme der Leistungsfähigkeit.

Des Weiteren wurde festgestellt, dass eine Reduzierung des Funktionsumfangs des Solid-Protokolls erforderlich ist, um eine sinnvolle Protokollausgabe zu ermöglichen. Der größte Eingriff in den Funktionsumfang war hierbei die Einschränkung der Autorisierungsoptionen, da bei nicht allen Autorisierungsvarianten eine Ermittlung des Anwendungskontexts möglich ist.

Chapter 5. Fazit

Eine Zugriffskontrolle, die einzelne Ressourcenzugriffe überwacht und als Protokoll für den Benutzer bereitstellt, ist eine notwendige Funktion für das Solid-Ökosystem. Eine Rückverfolgung der Zugriffe auf individueller Ebene ist eine wichtige Maßnahme, um das Vertrauen in die Freigabe von Ressourcen zu stärken, was ein wesentlicher Bestandteil von Solid ist. Es wäre wünschenswert, eine anbieterunabhängige Lösung zu finden, die auf den Mitteln des Solid-Ökosystems basiert. Allerdings hat sich gezeigt, dass zumindest die implementierte Variante eine zu hohe Netzwerklast erzeugt. Eine in den Anbieter integrierte Lösung könnte diese Leistungseinbußen ggf. umgehen und damit ebenfalls die Anwendungsfälle eines Datenschutzcockpits ermöglichen.