BÜRGERFREUNDLICHE ÜBERWACHUNG MIT EINER BLINDEN BLOCKCHAIN-DURCHLAUFSTELLE ZUR VORRATSDATEN-SPEICHERUNG MITTELS QUICK FREEZE

Karl Pinter / Dominik Schmelz / Markus Gruber / Thomas Grechenig

Karl Pinter, TU Wien, Institute of Information Systems Engineering, Research Group for Industrial Software (INSO)
Wiedner Hauptstraße 76/2, 1040 Wien, AT
karl.pinter@inso.tuwien.ac.at; https://www.inso.tuwien.ac.at

Dominik Schmelz, TU Wien, Institute of Information Systems Engineering, Research Group for Industrial Software (INSO)
Wiedner Hauptstraße 76/2, 1040 Wien, AT
dominik.schmelz@inso.tuwien.ac.at; https://www.inso.tuwien.ac.at

Markus Gruber, TU Wien, Institute of Information Systems Engineering, Research Group for Industrial Software (INSO)
Wiedner Hauptstraße 76/2, 1040 Wien, AT
markus.gruber@inso.tuwien.ac.at; https://www.inso.tuwien.ac.at

Thomas Grechenig, TU Wien, Institute of Information Systems Engineering, Research Group for Industrial Software (INSO)
Wiedner Hauptstraße 76/2, 1040 Wien, AT
thomas.grechenig@inso.tuwien.ac.at; https://www.inso.tuwien.ac.at

Schlagworte: ***Vorratsdaten, Überwachung, Datenkapitalismus, Tracking, Blockchain, Legal Tech***

Abstract: *Die Richtlinie 2006/24/EG regelte den Eingriff in die Telekommunikation aller Bürgerinnen und Bürgern innerhalb der EU. In diesem Zusammenhang sollten Metadaten anlasslos und flächendeckend gespeichert werden. Neben rechtlichen Bedenken schaffte dies auch ein Missbrauchspotenzial und Unbehagen. Die Autoren schlagen daher eine Lösung vor, die einerseits die Speicherung der geforderten Metadaten ermöglicht, andererseits aber auch ein gewisses Maß an Datenschutz gewährleistet. Es wird ein Prototyp vorgestellt, der mit Hilfe der Blockchain-Technologie das Missbrauchspotenzial reduziert und so zu einer rechtssicheren Überwachung im positiven Sinne beitragen könnte.*

1. Einführung und Motivation

Die Idee zu dem hier vorgestellten Prototypen wurde durch die Anschläge vom 11. September inspiriert, die sich im Jahr 2021 zum 20. Mal jährten. Eine der vielen Folgen war die Ausweitung der Überwachungsmaßnahmen auf globaler Ebene.[1]

Nach dem Sturz Napoleons bemühte sich Klemens Fürst Metternich um die Wiederherstellung der alten Fürstenstaaten in Österreich. Die eingesetzten Mittel waren für die damalige Zeit modern. Überwachungsmaßnahmen und Zensur wurden eingeführt, um die eigene Macht zu sichern. 1833 wurde das „Mainzer Informationsbüro" gegründet – der Geheimdienst der damaligen Zeit. Informelle Mitarbeiterinnen und Mitarbeiter stellten Daten zusammen.[2] Am Ende konnte die umfassende und anlasslose Überwachung nicht aufrechterhalten werden und endete in einer Revolution im Jahr 1848.[3]

[1] Arends, Surveillance in the post 11 september 2001 era, 2008.
[2] Adams, Historical Dictionary of German Intelligence, 2009, Seite xv.
[3] Adams, Historical Dictionary of German Intelligence, 2009, Seite xv.

Die Enthüllungen von Edward Snowden haben den Bürgerinnen und Bürgern deutlich gezeigt, dass die „Five Eyes“[4] permanent in ihre Privatsphäre eingreifen.[5] Unter anderem aus den historischen Ereignissen des 19ten Jahrhunderts lässt sich schließen, dass staatliche Überwachungsmaßnehmen keine neue Erfindung darstellen, sondern schon immer von Herrschenden eingesetzt wurden.

Eine Ausprägung von Überwachung, die in die Privatsphäre von Bürgerinnen und Bürgern eindringt und daher polarisiert, ist die Vorratsdatenspeicherung. Die Vorratsdatenspeicherung, wie sie in der Richtlinie 2006/24/EG vorgesehen war, schreibt einen Eingriff in die Kommunikation vor.[6] Die Richtlinie entstand im Lichte der Terroranschläge von Madrid und London[7], letzterer wird explizit in den Erwägungsgründen angeführt. Bei den Terroranschlägen von Madrid 2004 kamen 191 Menschen ums Leben.[8] In London kam es 2005 im U-Bahnnetz zu Anschlägen durch Selbstmordattentäter, 56 Personen inklusive der Attentäter wurden getötet.[9] Die Anschläge zeigten, wie schwierig eine verlässliche Früherkennung von Terrorismus sein kann.[10]

Metadaten der Kommunikation der Bürgerinnen und Bürger sollten laut Richtlinie 2006/24/EG flächendeckend und anlasslos gespeichert werden. Die öffentliche Diskussion darüber war kontrovers.[11] Die Speicherung selbst findet beim jeweiligen Anbieter statt. Der Gesetzgebungsprozess in den verschiedenen EU-Mitgliedstaaten wurde von einer öffentlichen Diskussion begleitet. In Österreich wurden zahlreiche Stellungnahmen abgegeben.[12] Nach einer Überprüfung dieser Stellungnahmen durch die Autoren zeigte sich, dass gerade auch Urheberrechtsverbände von dieser Möglichkeit zur Rückmeldung Gebrauch machten. Dies führte sofort zu der Frage, ob die Begehrlichkeit der Daten von anderen Interessen als dem Terrorismus getrieben ist. Laut Medienberichten wurde die Vorratsdatenspeicherung 2011 von Staatsanwaltschaften auch als Instrument zur Verfolgung von kleineren Delikten verwendet.[13] In einer Anfragebeantwortung der Justizministerin vom Jahr 2013 wurden die Delikte auf Grund derer abgefragt wurde aufgeschlüsselt.[14] Es handelte sich vorrangig um Diebstahl, Suchtgifthandel und beharrliche Verfolgung. Es schien, dass die Vorratsdatenspeicherung aufgrund höchstrichterlicher Entscheidungen des Gerichtshofs der Europäischen Union[15] und des Verfassungsgerichtshofs (VfGH) nie zur Anwendung kommen würde.[16]

Im Jahr 2018 wurde seitens der Politik das „Sicherheitspaket“ vorgestellt. Dieses sah vor, dass Daten bis zu einem Jahr gespeichert werden müssen, aber nur auf Anordnung der Staatsanwaltschaft.[17]

Das heißt aber auch, dass es keiner richterlichen Anordnung bedarf.[18] Dies entspricht zwar nicht der ursprünglich geplanten Form der Vorratsdatenspeicherung, die Ähnlichkeiten sind jedoch nicht von der Hand zu weisen. Die Speicherpflicht würde sich auf Verkehrs-, Zugangs- und Standortdaten beziehen.[19] Diese müssten von den Telekommunikationsanbietern gespeichert werden.

---

4 Allianz von Geheimdiensten (Australien, Kanada, Neuseeland, Vereinigtes Königreich und Vereinigten Staaten).
5 West, Historical Dictionary of International Intelligence, 2015, Seite xxvi.
6 Tschohl, Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung in Österreich, 2011, Seite 33ff.
7 West, Historical Dictionary of International Intelligence, 2015, Seite xxv.
8 Bundeszentrale für politische Bildung, 10 Jahre Terroranschläge von Madrid, 2014.
9 The Stationery Office, Report of the Official Account of the Bombings in London on 7th July 2005, 2006.
10 Denng, neue Bedrohungsformen Terrorismus – quo vadis?, 2011.
11 ORF, Privatsphäre ade, 2012.
12 Österreichisches Parlament, Stellungnahmen Telekommunikationsgesetz 2003, 2009.
13 Möchel, Vorratsdaten: Österreich legt sich quer, 2011.
14 Österreichisches Parlament, Anfragebeantwortung Steinhauser, 2013.
15 Gerichtshof der Europäischen Union, Urteil vom 8. April 2014, EU:C:2014:238.
16 Oesterreich.gv.at, Begriffslexikon, 2021.
17 Epicenter.Works, Überwachungspaket, 2021.
18 Epicenter.Works, Stellungnahme zum Ministerialentwurf betreffend eines Bundesgesetzes, mit dem die Strafprozessordnung 1975, das Staatsanwaltschaftsgesetz und das Telekommunikationsgesetz 2003 geändert werden (Strafprozessrechtsänderungsgesetz 2018 – 17 d.B. XXVI. GP, 2018, Seite 18.
19 Ebd., Seite 19.

In der Zwischenzeit gab es weitere Vorstöße in Richtung Vorratsdatenspeicherung auf EU-Ebene.[20] Immer wieder wurden weitere Forderungen gestellt.[21]

Die ePrivacy-Richtlinie aus dem Jahr 2002 soll in den nächsten Jahren durch die ePrivacy-Verordnung abgelöst werden. Die Vorratsdatenspeicherung wird in den Erwägungsgründen erwähnt.[22] Durch die Durchsicht der Historie lässt sich sagen, dass das Thema immer wieder ins Rampenlicht gerückt wird.

Im Jahr 2021 hat der EuGH die Vorratsdatenspeicherung in Estland eingeschränkt.[23] Es ist jedoch nicht klar, welcher Spielraum noch genutzt werden könnte, um die Vorratsdatenspeicherung wie ursprünglich geplant zu ermöglichen.[24] Klar ist, dass die Zukunft der Vorratsdatenspeicherung in der EU eine ungewisse ist.[25] In den aktuellen Schlussanträgen des Generalanwalts wird wiederholt, dass die Vorratsdatenspeicherung ausschließlich im Falle von ernsten Bedrohungen erlaubt sei und die Fragen bereits beantwortet oder aus der Rechtsprechung abzuleiten seien.[26]

2. Problemstellung

In § 135 Abs 2b Strafprozeßordnung (StPO) ist geregelt, dass eine Anlassdatenspeicherung unter bestimmten Bedingungen zulässig ist.

Ausgehend davon entwickelten die Autoren einen Prototypen für Anlassdatenspeicherung („quick freeze“) mittels einer Durchlaufstelle mit folgenden Eckdaten:

- Derzeit wird kein bestimmtes Werkzeug für eine Anlassdatenspeicherung vorgeschrieben. Das ist wenig verwunderlich, hat aber zur Folge, dass alle Provider und Behörden unterschiedliche Werkzeuge verwenden könnten. Ein Ziel ist es daher, ein einheitliches und übersichtliches Werkzeug zur Verfügung zu stellen.
- Eine Verbindung zwischen Anfrager (Behörde) und Auskunftgeber (Provider) könnte einfach hergestellt werden. Ziel ist es, einen sicheren Datentransfer zu ermöglichen. Die Durchlaufstelle ist blind und kann die transferierten Inhalte nicht sehen.
- Es muss klar geregelt sein, wer Anfragen stellen und wer Auskunft geben darf.
- Eine Nachvollziehbarkeit muss zu jedem Zeitpunkt gegeben sein.
- Die Daten, die gegebenenfalls ausgehändigt werden, sind per se vorhanden. Es müssen keine neuen Datenkategorien eingeführt werden. Nach einer Anordnung zur Anlassdatenspeicherung dürfen die gespeicherten Daten nicht gelöscht werden („quick freeze“).
- Eine blinde Durchlaufstelle[27] ist ein gutes Grundgerüst, muss jedoch um die Möglichkeit einer vertrauensstiftenden Technologie erweitert werden.
- Der Prototyp muss modernen Techniken entsprechen.

Eine Anlassdatenspeicherung („quick freeze“) wird in diesem Zusammenhang von den Autoren als „bürgerfreundlich“ bezeichnet. Damit ist gemeint, dass der staatliche Eingriff weniger intensiv als bei einer flächendeckenden und vor allem anlasslosen Speicherung von Vorratsdaten zu verstehen wäre. Die „Bürgerfreundlichkeit“ wird durch die oben angeführten Punkte wie Nachvollziehbarkeit und Übersichtlichkeit, vervollständigt. „Bürgerfreundlich“ und Anlassdatenspeicherung werden in Medienberichten immer wieder

[20] Möchel, Neue EU-Vorratsdatenspeicherung auf Initiative Österreichs, 2019.
[21] Möchel, EU-Ministerrat verlangt ‘gezielte Vorratsdatenspeicherung’, 2020.
[22] Möchel, E-Privacy-Verordnung erlaubt Vorratsdaten und Nachschlüssel, 2021.
[23] Möchel, EuGH-Urteil bremst neue Vorratsdatenpläne aus, 2021.
[24] Epicenter.Works, Vorratsdatenspeicherung, Standortdaten, Cookiebanner: die E-Privacy-Verordnung kommt, 2021.
[25] Rojszczak, The uncertain future of data retention laws in the EU: Is a legislative reset possible?, 2021.
[26] Gerichtshof der Europäischen Union, Pressemitteilung Nr. 206/21, 2021.
[27] Schafferer et al., Data retention services with soft privacy impacts: Concept and implementation, 2014, S. 178–181.

in Zusammenhang gebracht.[28] „Bürgerfreundliche Überwachung“, analog manchen Smart Cities in China[29], ist im weiteren Verlauf nicht gemeint.

Es ist klar, dass der Begriff unterschiedlich verstanden und sicherlich auch individuell definiert werden kann. Daher wird bereits in Folgearbeiten von den Autoren versucht, sich der Definition einer bürgerfreundlichen Überwachung anzunähern.

3. Prototyp

Die Autoren entwickelten einen Prototypen, der den oben beschriebenen Anforderungen genügt und im Folgenden beschrieben wird.

3.1. Durchlaufstelle

Haryadi et al. beschäftigten sich mit der Administration und Verwaltung von Systemen zur Vorratsdatenspeicherung.[30] Tschohl untersuchte die rechtlichen Rahmenbedingungen der Vorratsdatenspeicherung im speziellen in Österreich.[31] Das Konzept einer Durchlaufstelle wurde in einer Studie weiter untersucht und dargestellt.[32] Eine Durchlaufstelle dient als Schutz gegen unbefugte Teilnehmerinnen und Teilnehmer.

Schafferer et al. stellten eine mögliche technische Lösung auf Basis einer blinden Durchlaufstelle vor.[33,34] Technologien wie Blockchain oder DID (Dezentralised Identity) wurden dabei nicht genutzt, diese werden durch den hier vorgestellten Prototypen ergänzt.

3.2. Rollenbeschreibung

Der vorgestellte Prototyp besitzt folgende Rollen:

- Behörde (Authority): Eine befugte Stelle, die Anfragen an einen Provider stellen darf. Das können zum Beispiel Staatsanwaltschaften sein.
- Provider: Ein Internet Service Provider, der eine Anlassdatenspeicherung durchführen kann.

Aus rein technischer Sicht ergeben sich folgende Akteure, die sich an den Vorgaben laut W3C[35] orientieren:

- DLS User: Der Personenkreis, der sich am DLS authentifiziert. Das sind Behörde, Provider und Issuer. Der DLS User entspricht dem „holder“ und „subject“ laut W3C.[36]
- Issuer: Die Autorität, die festlegt, wer Provider und Behörde ist. Dieser entspricht dem „issuer“ laut W3C: „Issuers can issue verifiable credentials about any subject.“[37]
- DAapp Browser: Browser mit Wallet Integration. Praktisch werden alle einschlägigen Browser unterstützt.

[28] Knoke, „Mit ‚Quick Freeze’ droht ein Überwachungsstaat“, 2015.
[29] Mansmann, Smart Cities in China. Bürgerfreundliche Überwachung., 2016, S. 84.
[30] Haryadi et al., Lawful interception data retention regulation recommendation: Recommendations for countries that do not have relevant regulations of this field, 2011, S. 81–85.
[31] Tschohl, Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung in Österreich, 2011.
[32] Tschohl, Datensicherheit TKG Novelle 2010, 2011, S. 48ff.
[33] Schafferer et al., Data retention services with soft privacy impacts: Concept and implementation., 2014, S. 178–181.
[34] Schafferer et al., Implementing privacy sensitive governmental systems based on the concept of the Austrian data retention exchange service. 2014, S. 1–10.
[35] W3C, Verifiable Credentials Data Model 1.1, 2021.
[36] Ebd.
[37] Ebd.

- DID (Dezentralised IDentity) Provider: Dieser entspricht der „verifiable data registry“ laut W3C[38]. Hier bietet sich das European Blockchain Services Infrastructure (EBSI) an.[39]
- DApp (dezentrale Applikation): Web Applikation mit web3.js. Dies ist für den Zugriff auf lokal gespeicherte private keys in Wallets nötig (zum Beispiel Metamask).
- Audit Log: ein mittels Blockchain abgesicherter, unveränderlicher Speicher.
- Notary Service: Ein Dienst der Zeit und Hash eines Dokuments auf der Blockchain sicher ablegt und eine Überprüfung dessen erlaubt, um die Integrität von Daten zu gewährleisten.

3.3. eIDAS

Durch eIDAS (electronic IDentification, Authentication and trust Services) wurde die Möglichkeit geschaffen, innerhalb der Europäischen Union auf elektronischen Weg sicher und schnell zu kommunizieren.[40] Ein Ziel dabei ist, dass die nationalstaatlichen elektronischen Identitäten in allen Mitgliedsstaaten verwendet werden können.[41] Der vorliegende Prototyp bedient sich der eIDAS Vorgaben.

3.4. EBSI (European Blockchain Service Infrastructure)

Die Initiative der Europäischen Kommission und der EPB (European Blockchain Partnership) hat zum Ziel, grenzüberschreitende Dienste für die öffentliche Verwaltung anzuregen und zu ermöglichen.[42] Dabei werden offene Standards explizit unterstützt. Abbildung 1 zeigt einen Verifikationsprozess nach Pastor («What is EBSI»).

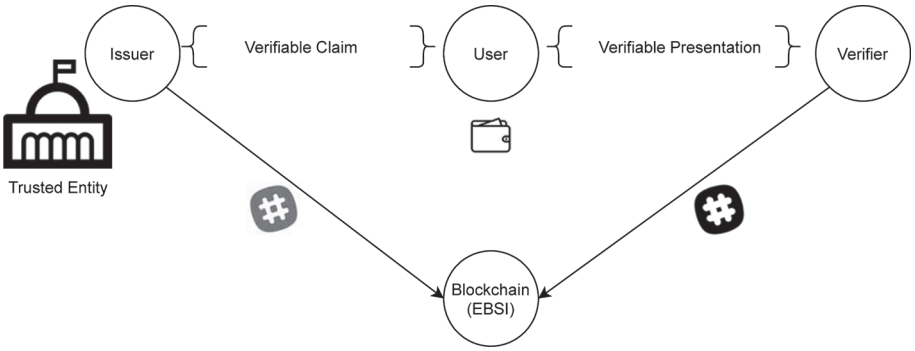

Abbildung 1

3.5. Blockchain als Stamping Service

Die Blockchain ermöglicht eine transparente, unveränderliche, dezentrale Speicherung von Daten. Blockchain wird inflationär, oft technisch ungerechtfertigt in Anwendungsfällen, in welchen eine klassische zentrale Datenbank besser wäre, verwendet. Im gegenständlichen Fall entschieden sich die Autoren bewusst für eine Blockchain Anwendung, da die Teilnehmerinnen und Teilnehmer gegensätzliche Interessen besitzen und eine gemeinsame Datenhaltung mit den zuvor genannten Eigenschaften den Anwendungsfall unterstützen.

[38] Ebd.
[39] CEF Digital, European Blockchain Services Infrastructure (EBSI), 2021.
[40] European Commission, Discover eIDAS, 2021.
[41] Oesterreich.gv.at, Elektronische Identität (eID) anderer EU-Mitgliedstaaten, 2021.
[42] Pastor, What is EBSI?, 2021.

Das vom Prototypen benutzte Stamping Service dient als Existenznachweis und Integritätsnachweis (Zeit und Fingerabdruck). So kann überprüft werden, ob Daten im Nachhinein verändert wurden und wann Abfragen durch wen angestoßen und beantwortet wurden.

3.6. Anlassdatenspeicherung

Bildet man das Prinzip der Anlassdatenspeicherung in stark vereinfachter Form ab, so ergibt sich das folgende Bild (Abbildung 2). Die Behörde fragt beim jeweiligen Anbieter von Telekommunikationsdiensten an und kann Daten dort beauskunften lassen. Der Prototyp erweitert die hier simplifiziert dargestellte Form.

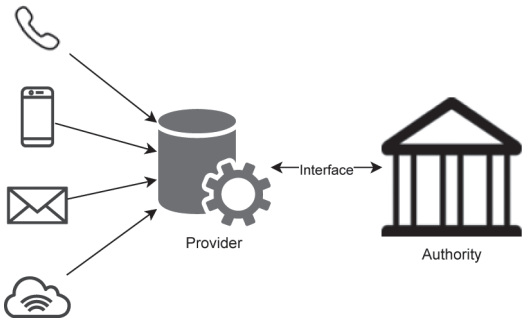

Abbildung 2

3.7. Architektur

Die europäische Union entwickelt seit 2018 in ihrer European Blockchain Partnership (EBP) eine dezentrale Authentisierungsplattform namens ESSIF (European Self Sovereign Identities Framework), welche es erlaubt Self Sovereign Identities (SSI) zu erstellen und diese in registrierten Applikationen zu integrieren.[43] Dazu erstellt, wie in Abbildung 1 dargestellt, ein Issuer eine eIDAS kompatible verifizierbare Identität und übergibt sie dem User. Dabei ist zu beachten, dass sich das tatsächliche Schlüsselmaterial, welches zur kryptographischen Authentisierung verwendet wird, nur beim User befindet und der Issuer diese tatsächlich nur bestätigt. Der User kann dann diese verifizierbare Identität einem Dritten (Verifier) vorweisen. Auch ist es möglich, einzelne Attribute, wie Geburtsdatum oder Namen, bestätigen zu lassen. Der ESSIF Decentralized Identifier (DID) wird verwendet, um einen sicheren Datenaustausch zwischen der Berhöde und den Providern zu ermöglichen.

Abbildung 3 zeigt die Abfolge des Antrags und dessen Beantwortung. Zuerst authentifiziert sich der User gegenüber der Plattform (1–2) und ruft die Antragsmaske ab (3–4). Diese beinhaltet die Liste der verfügbaren Provider. Nach Auswahl des Providers und Angabe der notwendigen Daten wird die DID des Providers abgerufen, inklusive seines öffentlichen Schlüssels (5–6). Mithilfe des privaten Schlüssels des Users wird der Antrag signiert und mit dem öffentlichen Schlüssel des Providers verschlüsselt. Damit ist die Integrität, Authentizität und Vertraulichkeit des Antrags gewährleistet. Dieser Antrag wird an die Plattform gesendet (7). Dort wird er in einem unveränderlichen, durch auf der Blockchain abgelegten Fingerabdruck abgesicherten Storage, abgelegt. Der Vorgang wird in einem wiederum gegen Veränderungen abgesicherten Audit-Log abgelegt.

[43] Pastor, What is EBSI?, 2021.

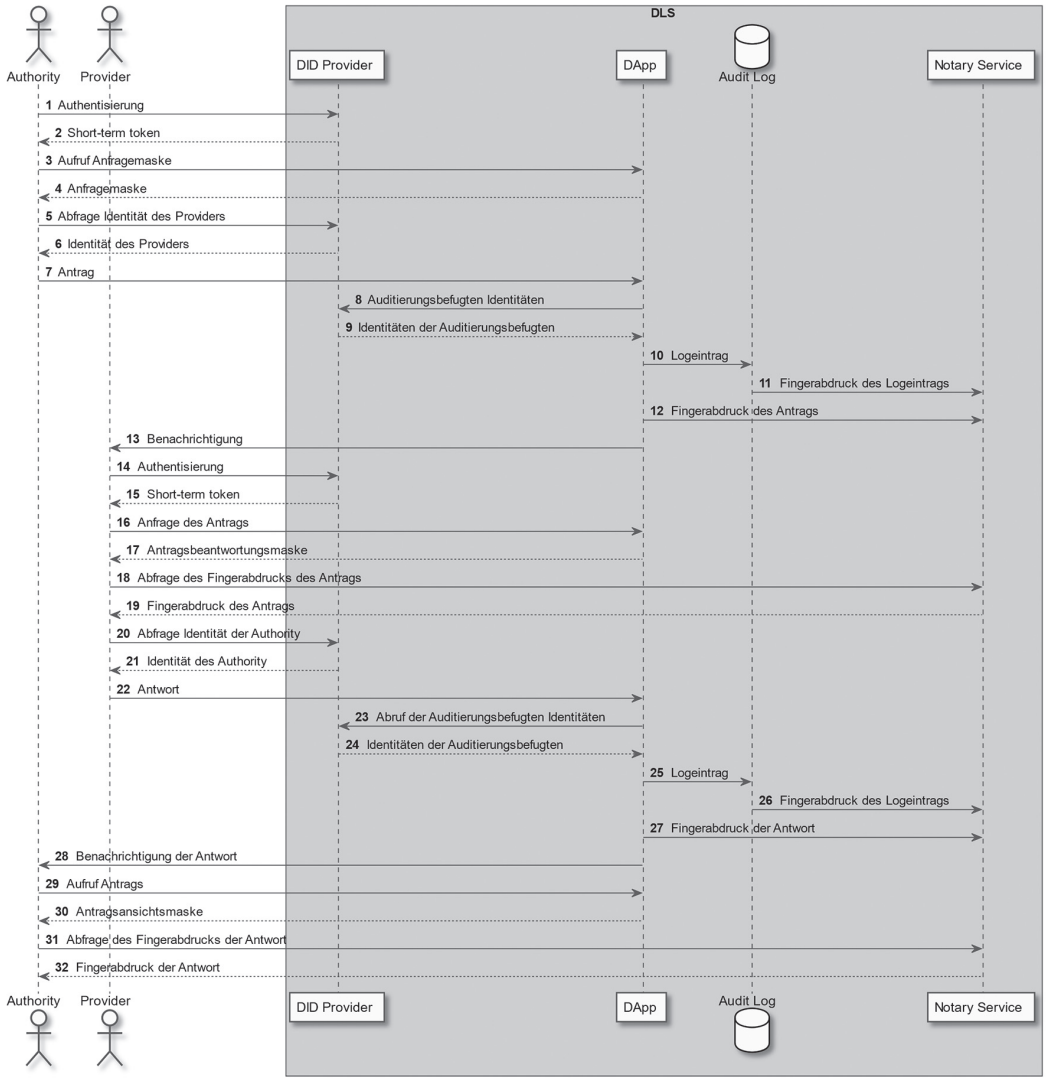

Abbildung 3

Dieser Log Eintrag wird mit allen öffentlichen Schlüsseln, der zur Auditierung berechtigten (Auditoren) hybrid, verschlüsselt, also die Daten mit einem symmetrischen Schlüssel verschlüsselt, welcher dann jeweils mit den asymmetrischen Schlüsseln verschlüsselt wird (8–12). Damit kann jeder der Auditoren die Einträge im Falle eines Audits entschlüsseln und deren Integrität prüfen. Der Provider wird von dem Antrag informiert (13) und kann diesen nach erfolgreicher Authentifizierung (14–15) einsehen (16–17) und mit seinem privaten Schlüssel entschlüsseln. Die Fingerabrücke des Antrags werden geprüft (18–19). Der Provider sucht die angefragten Daten in seinem eigenen System und packt sie in ein Dokument oder Archiv. Die angefragten Daten kann der Provider mithilfe der Maske wiederum mit dem öffentlichen Schlüssel des Antragstellers verschlüsseln und mit dem privaten Schlüssel des Providers signieren. Diese Daten werden, wie die Anträge selbst auch, an die Plattform gesendet (20–22) und unveränderlich abgelegt und ein Audit-Logeintrag erstellt (23–27). Der Antragsteller wird über die Beantwortung seiner Anfrage informiert (28) und kann diese mittels

der Plattform einsehen und entschlüsseln (29–30). Nach erfolgreicher Entschlüsselung wird die Signatur der Daten geprüft, um die Authentizität und Integrität der Daten zu überprüfen (31–32).

Im Falle eines Entschlüsselungs- oder Integritätsfehlers kann der Antrag erneut gestellt oder eskaliert werden. Ein Eskalationsprozess ist nicht Teil des Prototypen.

Durch die Verwendung der Blockchain konnte der existierende Prozess weiter abgesichert werden. Speziell wurden Identitäten in einer öffentlichen Blockchain gespeichert und zur Authentifizierung und Verschlüsselung verwendet. Weiters wurde die Blockchain zur Speicherung der Fingerabdrücke der Anträge, Antwortdaten und Auditlogeinträgen verwendet.

4. Schlussfolgerungen

Das Problem einer anlasslosen und flächendeckenden staatlichen Überwachung wurde in Österreich viel diskutiert. Die politische Diskussion dauert weiter an. Menschliche oder technische Fehler bei der Speicherung, Abfrage oder Auswertung können naturgemäß bei keinem System ausgeschlossen werden. Ein Ziel beim Bau eines derartigen Prototypen ist es, die Missbrauchs- und Fehlergefahr einzudämmen. Der Prototyp ist blind und verwendet aktuelle Technologien wie DID oder EBSI, um ein Maximum an Sicherheit und Nachvollziehbarkeit zu gewährleisten.

Die vollständig digitale Verarbeitung erlaubt eine Fehlervermeidung und Nachvollziehbarkeit. Die Fehlervermeidung von digitalen Prozessen resultiert einerseits durch Vermeidung von Medienbrüchen und andererseits durch technische Mechanismen. Ein unautorisierter Antrag, also ein Antrag von einer dritten, nicht berechtigten Person wird durch die Authentisierung und kryptographische Signatur vermieden. Eine kryptographische Signatur ist wesentlich schwerer zu fälschen als eine analoge Signatur und kann technisch überprüft werden. Dadurch kann technisch vermieden werden, dass jemand nicht Autorisierter einen Antrag gegenüber einem Provider stellt.

Weiters wird durch die Signatur und die Anwendung von Blockchain-Technologie eine Veränderung des Antrages technisch vermieden. Eine Veränderung würde einerseits beim Abgleich des Fingerabdrucks auf der Blockchain auffallen und andererseits die bereits genannte Signatur invalidieren. Somit kann ein Missbrauch durch Veränderung eines Antrages am Transportweg technisch vermieden werden.

Durch die Nachweisbarkeit über das Audit-Log ist ein Missbrauch bzw. ein Fehler nachvollziehbar. Dieses Audit-Log kann im Falle eines Vorfalles oder Verdachts durch den Auditor eingesehen werden. Dieses Audit-Log ist gegen Manipulation mittels der Blockchain-Technologie abgesichert. Selbst der Systembetreiber könnte, zum Beispiel bei veränderter politischer Lage, keine Veränderungen vornehmen. Dadurch kann sowohl Missbrauch als auch etwaige Fehler in der Verarbeitung nachvollzogen werden.

Der Prototyp soll dazu beitragen, eine bürgerfreundliche, rechtskonforme Überwachung zu untersuchen. Mögliche Erweiterungen für zukünftige Forschung sind die dezentrale Speicherung der Daten und Applikation und die Implementierung von Fehler- und Eskalationsprozessen.

5. Literatur

Adams, Jefferson, Historical Dictionary of German Intelligence, Boston, Scarecrow Press, 2009.

Arends, Max, Surveillance in the post 11 september 2001 era, 2008.

Bundeszentrale für politische Bildung, 10 Jahre Terroranschläge von Madrid, https://www.bpb.de/politik/hintergrund-aktuell/180328/10-jahre-terroranschlaege-in-madrid-11-03-2014 (aufgerufen am 29.11.2021), 2014.

CEF Digital, European Blockchain Services Infrastructure (EBSI), https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI (aufgerufen am 13.09.2021), 2021.

Denng, Anton, neue Bedrohungsformen Terrorismus – quo vadis?, IFK Monitor Februar 2011, https://www.bundesheer.at/pdf_pool/publikationen/ifk_monitor_7_terror_quo_vadis_2011_ad.pdf (aufgerufen 29.11.2021), 2011.

Epicenter.Works, Stellungnahme zum Ministerialentwurf betreffend eines Bundesgesetzes, mit dem die Strafprozessordnung 1975, das Staatsanwaltschaftsgesetz und das Telekommunikationsgesetz 2003 geändert werden (Strafprozessrechtsänderungsgesetz 2018 – 17 d.B. XXVI. GP, https://epicenter.works/sites/default/files/epicenter.works_-_strafprozessanderungsg_2018_17_xxvi_gp-print.pdf, 2018.

Epicenter.Works, Überwachungspaket, https://epicenter.works/thema/ueberwachungspaket (aufgerufen am 02.10.2021).

Epicenter.Works, Vorratsdatenspeicherung, Standortdaten, Cookiebanner: die E-Privacy-Verordnung kommt, https://epicenter.works/content/vorratsdatenspeicherung-standortdaten-cookiebanner-die-eprivacy-verordnung-kommt (aufgerufen am 03.10.2021), 2021.

European Commission, Discover eIDAS, https://digital-strategy.ec.europa.eu/en/policies/discover-eidas (aufgerufen am 28.10.2021), 2021.

Gerichtshof der Europäischen Union, Pressemitteilung Nr. 206/21, Luxenburg, https://curia.europa.eu/jcms/upload/docs/application/pdf/2021-11/cp210206de.pdf (aufgerufen am 30.11.2021), 2021.

Gerichtshof der Europäischen Union, Urteil vom 8. April 2014, Elektronische Kommunikation – Richtlinie 2006/24/EG – Öffentlich zugängliche elektronische Kommunikationsdienste oder öffentliche Kommunikationsnetze – Vorratsspeicherung von Daten, die bei der Bereitstellung solcher Dienste erzeugt oder verarbeitet werden – Gültigkeit – Art. 7, 8 und 11 der Charta der Grundrechte der Europäischen Union, C-293/12 und C-594/12, EU:C:2014:238

Haryadi, Sigit/Malik, indira, Lawful interception data retention regulation recommendation: Recommendations for countries that do not have relevant regulations of this field. In 2011 6th International Conference on Telecommunication Systems, Services, and Applications (TSSA), 2011, S. 81–85.

Knoke, Felix, „Mit ‚Quick Freeze' droht ein Überwachungsstaat", https://www.spiegel.de/netzwelt/web/vorratsdatenspeicherung-mit-quick-freeze-droht-ein-ueberwachungsstaat-a-738708.html (aufgerufen am 9.12.2021), 2015.

Mansmann, Urs, Smart Cities in China. Bürgerfreundliche Überwachung., c't Magazin, 6/2016.

Möchel, Erich, E-Privacy-Verordnung erlaubt Vorratsdaten und Nachschlüssel, https://fm4.orf.at/stories/3011921 (aufgerufen am 24.09.2021), 2021.

Möchel, Erich, EU-Ministerrat verlangt 'gezielte Vorratsdatenspeicherung', https://fm4.orf.at/stories/3009144 (aufgerufen am 26.09.2021), 2020.

Möchel, Erich, EuGH-Urteil bremst neue Vorratsdatenpläne aus, https://fm4.orf.at/stories/3012490 (aufgerufen am 02.10.2021), 2021.

Möchel, Erich, Neue EU-Vorratsdatenspeicherung auf Initiative Österreichs, https://fm4.orf.at/stories/2975759 (aufgerufen am 28.09.2021), 2019.

Möchel, Erich, Vorratsdaten: Österreich legt sich quer, https://fm4v3.orf.at/stories/1682829/index.html, (aufgerufen am 30.11.2021), 2011.

Oesterreich.gv.at, Begriffslexikon, https://www.oesterreich.gv.at/lexicon/V/Seite.991898.html (aufgerufen am 12.10.2021), 2021.

Oesterreich.gv.at, Elektronische Identität (eID) anderer EU-Mitgliedstaaten, https://www.oesterreich.gv.at/themen/dokumente_und_recht/elektronische-identit%C3%A4t-(eiD)-anderer-eu-mitgliedstaaten-(SDG).html (aufgerufen am 14.10.2021), 2021.

ORF, Privatsphäre ade, https://orf.at/v2/stories/2113030/2113029/ (aufgerufen am 13.08.2021), 2012.

Österreichisches Parlament, Anfragebeantwortung Steinhauser, https://www.parlament.gv.at/PAKT/VHG/XXIV/AB/AB_14397/imfname_314525.pdf (aufgerufen am 30.11.2021), 2013.

Österreichisches Parlament, Stellungnahmen Telekommunikationsgesetz 2003, https://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00117/index.shtml (aufgerufen am 05.07.2021), 2009.

Pastor, Marta, What is EBSI?, https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=381517902 (aufgerufen am 14.10.2021), 2021.

Rojszczak, Marcin, The uncertain future of data retention laws in the EU: Is a legislative reset possible? In: computer law & security review 41, Elsevier BV, 2021.

Schafferer, Michael/Gruber, Markus/Schanes, Christian/Grechenig, Thomas, Data retention services with soft privacy impacts: Concept and implementation. In: 2014 IEEE 5th International Conference on Software Engineering and Service Science, 2014, S. 178–181.

Schafferer, Michael/Gruber, Markus/Grechenig, Thomas, Implementing privacy sensitive governmental systems based on the concept of the Austrian data retention exchange service. In: eChallenges e-2014 Conference Proceedings, 2014, S. 1–10.

The Stationery Office, Report of the Official Account of the Bombings in London on 7th July 2005, http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/11_05_06_narrative.pdf (aufgerufen 29.11.2021), 2006.

Tschohl, Christof, Datensicherheit bei der Umsetzung der Vorratsdatenspeicherung in Österreich, Wien, Thesis, 2011.

Tschohl, Christof, Datensicherheit TKG Novelle 2010, Studie: Datensicherheit in der TKG Novelle zur Umsetzung der Vorratsdatenspeicherung in Österreich, Ludwig Boltzmann Institut für Menschenrechte, 2011.

West, nigel, Historical Dictionary of International Intelligence, Lanham, Maryland, Rowman & Littlefield, 2015.

W3C, Verifiable Credentials Data Model 1.1, https://www.w3.org/TR/vc-data-model/ (aufgerufen am 26.11.2021), 2021.