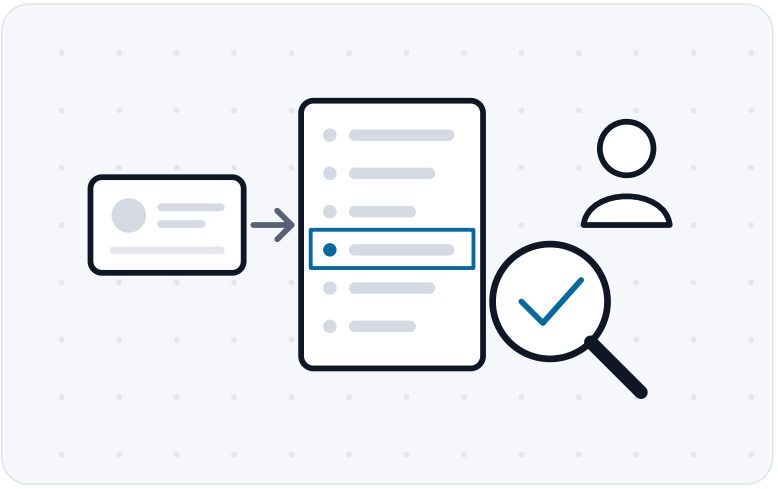
A-SIT Technology

E-Government Innovationszentrum

21. November 2024 Konzept · Transparenz · Digitale Identität · 29 Min. Lesezeit

Designüberlegungen von Ex-post-TETs für die Transparenz von Anmeldeinformationen

Edona Fasllija



Autorinnen und Autoren	Edona Fasllija
Quelle	https://technology2.a-sit.at/veroeffentlichungen/ex-post-tets-fuer-die-transparenz-von-anmeldeinformationen/
Hinweis	Maschinell übersetzt.

Kernaussagen

- Credential Transparency soll Ausstellung, Überprüfung und Widerruf von Nachweisen öffentlich prüfbar machen, ohne sensible Informationen preiszugeben.
- Ein CIT-Log-Eintrag besteht aus dem Hash des Nachweises und einem geblindeten Commitment an die UserID, sodass Benutzer eigene Einträge erkennen können.
- CIT-Log-Einträge sind konstant 96 Byte groß; bei der Wachstumsrate von CT entstünden 746 MB statt 43,99 GB neue Log-Daten pro Tag.
- CIT fügt bei der Vorlage von Nachweisen weniger als 2 Millisekunden Overhead hinzu; die Verifikation dauert weniger als 10 Sekunden.

> - Transparenz in allen Phasen (Wallet-Binärdateien, Ausstellung, Vorlage, Widerruf) stärkt Rechenschaftspflicht, Sicherheit und die Position der Benutzer.

Ex-post-Transparenztechnologien sollen betroffenen Personen helfen, ihr Recht auf Transparenz wahrzunehmen, indem sie ihnen Einblick in die sensiblen Daten geben, die gesammelt, verarbeitet oder an verschiedene Akteure weitergegeben werden. In diesem Projekt werden die wichtigsten Designüberlegungen bei der Entwicklung eines solchen Tools für digitale Ausweissysteme durchgespielt, angefangen bei maßgeschneiderten sicheren Protokollierungsmechanismen, Bereinigung, Abfrage-, Überwachungs- und Prüfmechanismen sowie externen Mechanismen, die mit den betroffenen Personen interagieren.

1. Einleitung

Die Verbreitung digitaler Identitätslösungen in Europa hat mit der Einführung der Europäischen Brieftasche für die Digitale Identität (European Digital Identity Wallet, EDIW) [1] und der aktualisierten eIDAS-2.0-Verordnung [2] an Dynamik gewonnen, die die ursprüngliche Verordnung über elektronische Identifizierung, Authentifizierung und Vertrauensdienste (eIDAS) erweitert. Diese Initiativen sollen europäischen Bürgerinnen, Bürgern und Einwohnerinnen und Einwohnern ein standardisiertes, interoperables und sicheres Mittel bieten, ihre Identität nachzuweisen und überprüfbare Nachweise (Verifiable Credentials) grenzüberschreitend zu teilen. Eine zentrale Herausforderung in diesem Ökosystem besteht darin, sicherzustellen, dass diese Nachweise vertrauenswürdig, manipulationssicher und transparent sind.

Transparency Enhancing Technologies (TETs) sind technische Lösungen, die Transparenz in Systemen oder Prozessen fördern sollen. Insbesondere „Ex-post"-TETs [3] liefern Informationen erst, nachdem ein Ereignis eingetreten ist, und ermöglichen so eine nachträgliche Analyse. Dieses Projekt befasst sich mit Entwurf, Entwicklung und Bewertung von Ex-post-TETs, die sich in verschiedene Systeme integrieren lassen, um nachweisbare Transparenz zu schaffen. Es wird veranschaulicht, wie TETs auf digitale Nachweissysteme angewendet werden können, um Benutzern Einblick zu geben und Vertrauen durch kryptografische Beweise zu fördern, dass Daten unverändert bleiben.

Konkret untersucht dieses Projekt die Designüberlegungen für die Umsetzung protokollbasierter TETs in nutzerzentrierten Frameworks für digitale Identität, mit Schwerpunkt auf Verifiable Credentials [4]. In diesem Kontext bilden protokollbasierte Transparenzsysteme eine Grundlage für manipulationssichtbare, überprüfbare Aufzeichnungen, die unabhängig geprüft werden können. Aufbauend auf Konzepten etablierter Transparenzsysteme wie Certificate Transparency und Key Transparency wird untersucht, wie Transparency Logs digitale Nachweise über den gesamten Lebenszyklus unterstützen können, einschließlich Ausstellung, Überprüfung, Nutzung und Widerruf. Jede Phase profitiert von Transparency Logs, die unabhängige Prüfbarkeit und Rechenschaftspflicht ermöglichen und zugleich die Privatsphäre der Benutzer wahren.

2. Ziele und Herausforderungen

Credential Transparency ist ein Konzept, das in diesem Bericht eingeführt wird, um einen datenschutzfreundlichen, prüfungsfreundlichen Rahmen für die Verwaltung und Überprüfung digitaler Nachweise zu beschreiben. Credential Transparency stellt sicher, dass jede Phase im Lebenszyklus eines Nachweises, etwa Ausstellung, Überprüfung oder Widerruf, öffentlich prüfbar nachverfolgt werden kann, ohne sensible Informationen preiszugeben. Credential Transparency soll Transparenz und Rechenschaftspflicht in Nachweissystemen stärken und zugleich die Privatsphäre der Benutzer wahren. Dieser Ansatz erfordert fortgeschrittene kryptografische Methoden, die es ermöglichen, die Echtheit und Gültigkeit eines Nachweises zu überprüfen, ohne sensible Informationen über den Benutzer offenzulegen.

Ein prominentes Beispiel für transparente Prüfprotokollierung ist Certificate Transparency (CT) [4], das die Machbarkeit und den Nutzen öffentlicher Logs zur Nachverfolgung von Zertifikaten belegt hat. Dieser Ansatz lässt sich jedoch wegen grundlegender Unterschiede bei den Datenschutzanforderungen nicht direkt auf digitale Nachweise übertragen. Anders als die vollständig öffentlichen Zertifikate in CT ist der Inhalt digitaler Nachweise privat. Würde ein vollständiger Nachweis wie bei Zertifikaten protokolliert, würden daher sensible Benutzerinformationen offengelegt, was Credential Transparency verhindern will.

Die Lösung liegt in einem Blinding-Mechanismus, der zwei zentrale Herausforderungen adressiert. Die erste ist die Auffindbarkeit für Benutzer (user discoverability): Ein Benutzer soll feststellen können, ob sein Nachweis mit einem bestimmten Eintrag im Nachweis-Log verknüpft ist. Die zweite ist die Überprüfbarkeit für Prüfer (verifier verifiability): Ein Prüfer (Verifier), dem ein Nachweis und ein zugehöriger Log-Eintrag vorgelegt werden, soll bestätigen können, ob der Log-Eintrag zu genau diesem Nachweis passt.

Zusätzlich zu diesen funktionalen Anforderungen muss Credential Transparency zwei entscheidende Datenschutzanforderungen erfüllen. Die erste ist Nachweis-Privatsphäre (credential privacy): Es soll praktisch unmöglich sein, aus dem öffentlichen Log-Eintrag Informationen über die Angaben (Claims) des Nachweises abzuleiten. Die zweite ist Nachweis-Unverkettbarkeit (credential unlinkability): Selbst wenn zwei verschiedene Nachweise und ihre Log-Einträge verglichen werden, soll es schwierig bleiben, daraus zu schließen, ob sie derselben Person gehören.

Indem Credential Transparency diese datenschutzfreundlichen Prinzipien einhält und die Herausforderungen der Auffindbarkeit und Überprüfbarkeit löst, soll der Nutzen öffentlicher Prüfbarkeit auf Nachweissysteme übertragen werden, ohne die Privatsphäre der Benutzer zu beeinträchtigen.

3. Hintergrund

3.1. Nachweissysteme

Ein Nachweis (Credential) ist eine von einer Instanz ausgestellte Aussage über einen Benutzer (oder Inhaber), die Attribute wie den Namen des Benutzers, körperliche Merkmale, Zugehörigkeiten oder andere überprüfte persönliche Angaben enthalten kann. Der Benutzer kann diesen Nachweis einem Prüfer (Verifier) vorlegen, der darauf vertrauen kann, dass der Benutzer die angegebenen Attribute besitzt, sofern er dem Aussteller vertraut. Die kombinierten Prozesse der Ausstellung und Vorlage eines Nachweises bilden ein sogenanntes Nachweisschema (Credential Scheme).

Herkömmliche Nachweisschemata sind in der Regel zentralisiert, wobei der Server des Ausstellers alle Benutzerinformationen vorhält. Im Gegensatz dazu erlauben nutzerzentrierte Ansätze für digitale Identität wie Self-Sovereign Identity (SSI) Einzelpersonen, ihre eigenen digitalen Bestätigungen von Identitätsattributen und kryptografische Schlüssel zur Authentifizierung selbst zu verwalten. Das geschieht häufig auf persönlichen Geräten wie Smartphones über eine „Wallet"-Anwendung. Diese Bestätigungen tragen einen kryptografischen Integritätsnachweis, in der Regel in Form einer digitalen Signatur des Ausstellers, wodurch die Informationen maschinell überprüfbar sind. Dieses Konzept hat den Begriff „Verifiable Credentials" (VCs) [5] für diese Bestätigungen hervorgebracht.

Datenschutzorientierte VPs erlauben selektive Offenlegung (Selective Disclosure), sodass Benutzer nur die notwendigen Attribute an den Prüfer weitergeben können. VPs enthalten außerdem kryptografische Belege, etwa geblindete Beweise (Blinded Proofs), die vom Nachweis stammen und bestätigen, dass die angezeigten Attribute tatsächlich aus einem von einer vertrauenswürdigen Instanz ausgestellten Nachweis stammen. Diese Beweise können mit verschiedenen Techniken erstellt werden, darunter Merkle-Hash-Bäume oder Zero-Knowledge-Beweise. Der Prüfer kann den Beweis dann automatisch validieren und bestätigen, dass der Nachweis von einem vertrauenswürdigen Aussteller ausgestellt wurde. Das sichert die Echtheit der vom Benutzer behaupteten Identitätsattribute und ermöglicht den Zugang zu Diensten.

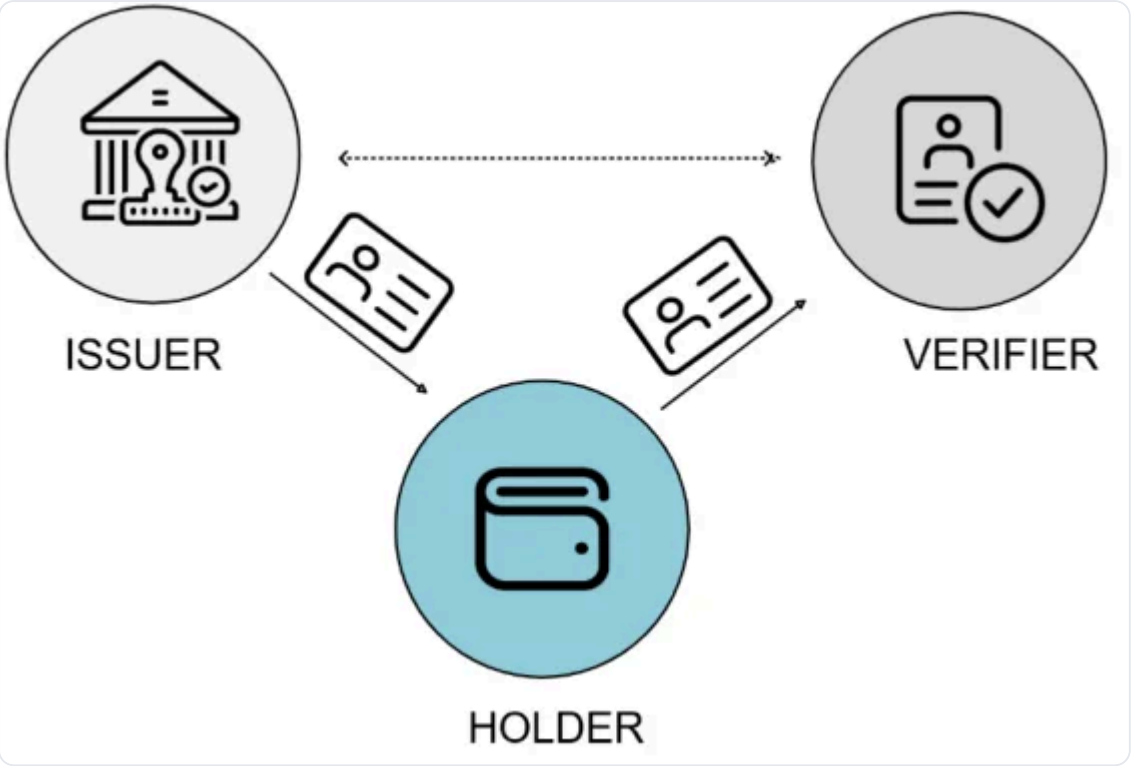


Abbildung 1: Vertrauensdreieck der Verifiable Credentials: Der Begriff Verifiable Presentation (VP) beschreibt den Vorgang, bei dem Benutzer bestimmte Identitätsattribute aus ihren Nachweisen gegenüber Prüfern offenlegen, die auch als Relying Parties bezeichnet werden. Erhält der Benutzer die Präsentationsanfrage, durchsucht seine digitale Wallet-App automatisch die gespeicherten Nachweise nach den angeforderten Attributen, die den Kriterien der Anfrage entsprechen. Mit Zustimmung des Benutzers erzeugt die Wallet-App einen kryptografischen Beweis für die Richtigkeit dieser Attribute und sendet Attribute und Beweis an den Prüfer.

3.2. Transparenzsysteme

Die Kernidee von Transparenzsystemen ist die öffentliche Aufzeichnung aller von einer Instanz ausgestellten Bestätigungen, was Sichtbarkeit und Rechenschaftspflicht fördert. Diese Transparenz erleichtert es, unbefugte oder betrügerische Handlungen dieser Instanzen zu erkennen. Eines der frühesten und am weitesten verbreiteten Transparenzsysteme ist Certificate Transparency (CT) [4], das entwickelt wurde, um Rechenschaftspflicht in das häufig schlecht verwaltete WebPKI-Ökosystem zu bringen. Zuletzt zeichnet sich ein Trend ab, CT-ähnliche Systeme auch für andere Anwendungen außerhalb von WebPKI einzusetzen, etwa „Key Transparency" für sichere Messaging-Dienste [6].

Transparenzsysteme beruhen in der Regel auf extern prüfbaren Datenstrukturen, die öffentlich überprüfbar sind und zwei Haupteigenschaften aufweisen: (i) Sie sind „append-only", das heißt, Daten können weder gelöscht noch verändert werden, und (ii) sie sind konsistent und bieten allen Benutzern eine einheitliche Sicht auf die Daten. Diese Eigenschaften stellen sicher, dass das System für eine gegebene Abfrage dieselben Ergebnisse liefert. Das stärkt Vertrauen und Integrität, weil es schwer wird, die Daten zu verändern oder falsch darzustellen.

Akteure im Ökosystem

Dieser Abschnitt beschreibt die wichtigsten Beteiligten, die typischerweise an Transparenzsystemen mitwirken.

Der Log-Betreiber (Log Provider) ist eine nicht vertrauenswürdige Instanz, die für die Pflege eines öffentlichen, nur anfügbaren Prüf-Logs (Audit Log) zuständig ist, das Informationseinheiten, sogenannte Log-Einträge, speichert. Seine Hauptaufgabe besteht darin, diese Daten zu speichern und öffentlich zugänglich zu halten. Diese Aufgabe wollen herkömmliche Akteure möglicherweise nicht übernehmen. Da der Log-Betreiber nicht vertrauenswürdig ist, hat er keinen Zugriff auf private Informationen und kann kryptografisch daran gehindert werden, Daten zu verändern oder zu entfernen.

Auditoren überwachen den Log-Betreiber, um sicherzustellen, dass er Informationen korrekt anfügt und eine konsistente globale Sicht aufrechterhält. Auditoren spielen eine Schlüsselrolle beim Erkennen unehrlichen Verhaltens des Log-Betreibers. Jeder Auditor kann feststellen und unwiderlegbar belegen, ob ein Log-Betreiber betrogen hat. Da jede Person der Öffentlichkeit ohne besonderen Zugang als Auditor auftreten kann, müssen Log-Betreiber davon ausgehen, dass ihre veröffentlichten Daten laufend überwacht und geprüft werden. Dieser Aufbau erzwingt zusammen mit einem sicheren Gossip-Protokoll zum Austausch von Log-Fingerprints ehrliches Verhalten des Log-Betreibers.

Monitore prüfen häufig die vom Log-Betreiber veröffentlichten Daten, um die interne Konsistenz der Struktur zu verifizieren. Indem sie bestätigen, dass der Log frei von Inkonsistenzen bleibt, helfen Monitore, Fehlverhalten aufzudecken. Sie prüfen einzelne Log-Einträge, um unzulässige Ausstellungen zu erkennen, und können auch als Log-Spiegel (Log Mirrors) dienen, die Benutzern Such- und Benachrichtigungsdienste bieten.

Schließlich sind Quellen (Sources) die Instanzen, die die Ereignisse erzeugen, welche in der vom Log-Betreiber verwalteten Datenstruktur erfasst werden. Endbenutzer, für die die Log-Einträge relevant sind, fragen den Log-Betreiber ab, um diese Informationen abzurufen.

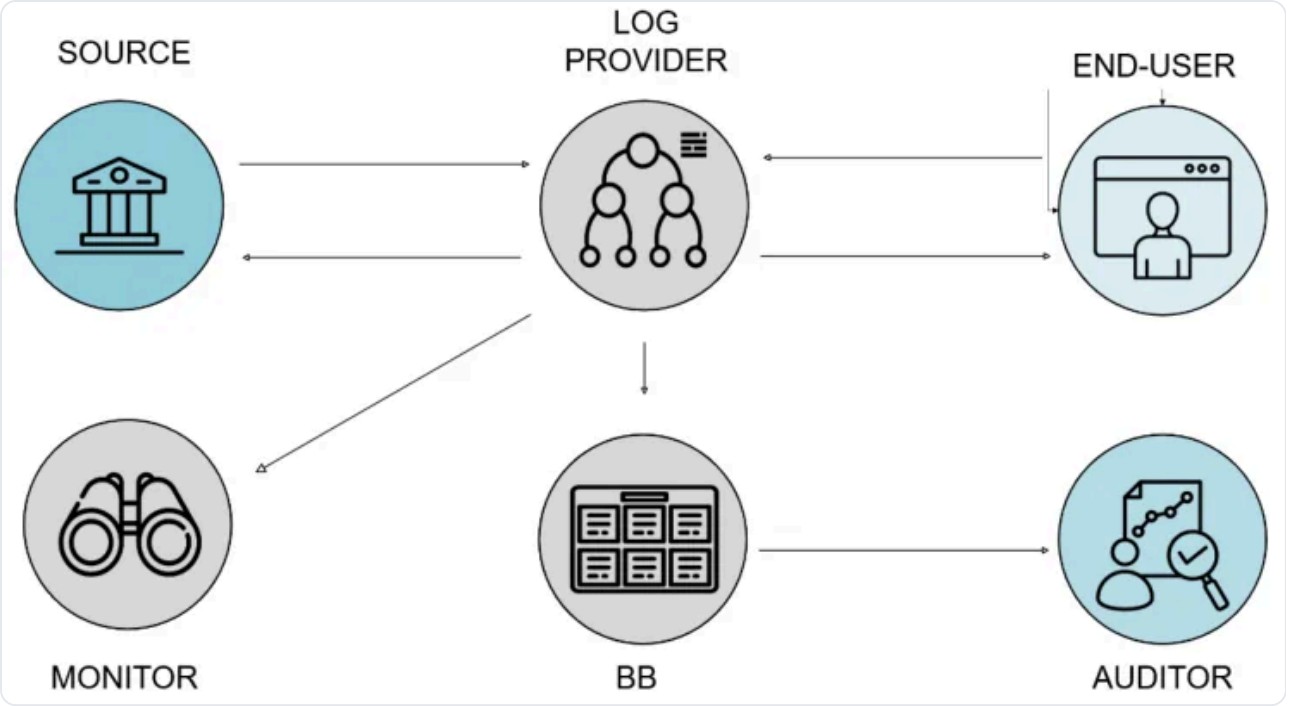


Abbildung 2: Überblick über Transparenzsysteme

3.3. Datenschutzfreundliche kryptografische Techniken

Zero-Knowledge-Beweise

Zero-Knowledge-Beweise (zk-Beweise) sind fortgeschrittene kryptografische Techniken, die es einem „Beweiser" (Prover) ermöglichen, einem „Prüfer" (Verifier) nachzuweisen, dass er bestimmte Informationen mit bestimmten Eigenschaften besitzt, ohne die Informationen selbst jemals preiszugeben. Dieser Ansatz ist besonders wertvoll in Szenarien, in denen Privatsphäre wesentlich ist, da er dem Prüfer die Gewissheit über das Wissen des Beweisers verschafft, ohne dass dieser sensible Daten offenlegen muss.

Unter den verschiedenen Arten von zk-Beweisen sind Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge (zkSNARKs) [7] besonders bemerkenswert. zkSNARKs sind kompakte Beweiskonstruktionen, die wiederholte Hin-und-her-Kommunikation zwischen Beweiser und Prüfer überflüssig machen. Diese nicht-interaktive Eigenschaft macht zkSNARKs effizient und skalierbar und ermöglicht schnellere Verifikationsprozesse, was in großen oder ressourcenbeschränkten Umgebungen entscheidend ist.

In dieser Arbeit werden zkSNARKs eingesetzt, um nachzuweisen, dass ein bestimmter datenschutzfreundlicher Eintrag in einem Transparency Log einer bestimmten datenschutzrelevanten Information entspricht und auf diese zurückgeführt werden könnte. Dadurch ist sichergestellt, dass zwar die Existenz des Eintrags und sein Zusammenhang mit bestimmten Informationen überprüfbar sind, die sensiblen Details selbst aber vertraulich bleiben. Diese Anwendung von zkSNARKs schafft einen wirkungsvollen Ausgleich zwischen Transparenz und Privatsphäre und stärkt das Vertrauen in Systeme, die auf datenschutzrelevanten Daten beruhen.

Blinding-Mechanismen

Blinding-Mechanismen in der Kryptografie sind Methoden, die bestimmte Informationen vor bestimmten Parteien verbergen und dabei ihre zugrunde liegende Echtheit oder Verwendbarkeit erhalten. Diese Techniken sind in datenschutzfreundlichen kryptografischen Systemen unverzichtbar, da sie Daten oder Identität verbergen und dennoch überprüfbar halten. Zu den wichtigsten Blinding-Mechanismen zählen Commitment-Funktionen und benutzerstabile Pseudonyme.

Commitment-Funktionen sind kryptografische Primitive, die es einem Benutzer (dem „Committer") erlauben, sich auf einen gewählten Wert oder eine Aussage festzulegen und diese vor anderen (dem „Empfänger") verborgen zu halten, mit der Zusicherung, dass der Wert später nicht mehr geändert werden kann. Dieser Prozess hat zwei Hauptschritte: (i) Commit-Phase: Der Committer wählt einen Wert und berechnet mit einer Commitment-Funktion ein Commitment, das eine Ausgabe erzeugt, die den ursprünglichen Wert verbirgt. Dieses Commitment wird dann an den Empfänger weitergegeben. (ii) Reveal-Phase: Will der Committer den verborgenen Wert offenlegen, gibt er sowohl den Wert als auch die beim Commitment verwendete Zufälligkeit bekannt. Der Empfänger kann überprüfen, ob der offengelegte Wert zum Commitment passt, indem er das Commitment neu berechnet und mit der ursprünglichen Commitment-Ausgabe vergleicht.

Commitment-Funktionen sind nützlich in Protokollen, in denen Vertrauen und Integrität erforderlich sind, etwa bei digitalen Wahlen oder Blockchain-Systemen. Sie bieten Eigenschaften wie Hiding, bei dem der ursprüngliche Wert geheim bleibt, und Binding, bei dem der Committer den Wert nach dem Commitment nicht mehr ändern kann.

Benutzerstabile Pseudonyme (User-Stable Pseudonyms) sind Kennungen, die Benutzern zugewiesen werden und über mehrere Interaktionen oder Sitzungen hinweg gleich bleiben, aber die reale Identität des Benutzers nicht direkt preisgeben. Dieser Mechanismus ermöglicht wiederholbare, authentifizierte Interaktionen, ohne die Privatsphäre des Benutzers zu beeinträchtigen. In der Praxis werden benutzerstabile Pseudonyme mit kryptografischen Methoden wie Hashing oder schlüsselbasierten Pseudozufallsfunktionen erzeugt, wobei nur bestimmte vertrauenswürdige Parteien die zugrunde liegende Identität kennen oder sie mit dem Pseudonym verknüpfen können.

Benutzerstabile Pseudonyme können in Kontexten wie anonymen Umfragen, dezentralen Identitätssystemen und datenschutzfreundlicher Authentifizierung eingesetzt werden, in denen das Verhalten oder der Ruf einer Person nachverfolgbar sein muss, ohne ihre tatsächliche Identität offenzulegen. Sie schaffen einen Ausgleich zwischen Rechenschaftspflicht und Privatsphäre, indem sie die Nachverfolgbarkeit von Interaktionen unter einem gleichbleibenden Pseudonym erlauben und personenbezogene Daten verborgen halten.

4. Designüberlegungen

4.1. Sichere Protokollierungsmechanismen

Transparenz erfordert, dass Informationen nachvollziehbar und überprüfbar aufgezeichnet werden. Das geschieht häufig durch eine strukturierte, chronologische Aufzeichnung von Ereignissen, Aktionen oder Daten, die ein System verwendet. Eine solche Aufzeichnung könnte sogar die vollständige Historie jedes Datenpunkts oder Bytes in seinem aktuellen oder früheren Zustand erfassen. Zur Unterstützung von

Transparenz werden Protokollierungsmechanismen häufig auf authentifizierten Datenstrukturen und Transparenz-Overlays aufgebaut, etwa Merkle-Bäumen oder Blockchains. Diese Strukturen stellen sicher, dass Logs nicht nur append-only und überprüfbar, sondern auch abfragbar und konsistent sind. In diesem Aufbau erfüllen Logs wesentliche Kriterien, darunter: (i) Konsistenz (Consistency): Ein möglicherweise unehrlicher Log-Server kann verschiedenen Parteien keine unterschiedlichen, widersprüchlichen Versionen des Logs präsentieren. (i) Nicht-Beschuldigbarkeit (Non-frameability): Parteien können einen Log-Server nicht für Fehlverhalten verantwortlich machen, wenn er tatsächlich ehrlich gehandelt hat. (i) Rechenschaftspflicht (Accountability): Es werden Belege bereitgestellt, um Log-Server zur Verantwortung zu ziehen, wenn sie Ereignisse nicht wie zugesagt aufnehmen. Durch die Kombination dieser Eigenschaften ermöglichen Transparency Logs ein vertrauenswürdiges System zur Nachverfolgung von Aktionen und Daten, das die Rechenschaftspflicht stärkt und vor Manipulation schützt.

Überprüfbare Datenstrukturen

Transparenzsysteme beruhen auf Datenstrukturen, die überprüfbare Beweise erzeugen und damit die Unveränderlichkeit und Integrität der Daten garantieren. Diese Strukturen unterscheiden sich in ihrem Aufbau, was sich auch auf die Arten von Beweisen auswirkt, die sie erzeugen können. Zudem beeinflusst die Datenstruktur die Effizienz von Operationen wie Lookups, Einfügungen und Prüfungen durch verschiedene Parteien, die entscheidende Kennzahlen für die Eignung einer Datenstruktur in Transparenzsystemen sind.

Überblick über überprüfbare Datenstrukturen und kryptografische Beweise

Der Entwurf der zugrunde liegenden Datenstruktur ist für Transparenzsysteme entscheidend, da er unmittelbar beeinflusst, ob das System seine zentralen Anforderungen an Sicherheit, Effizienz und Transparenz erfüllen kann. Im Folgenden werden einige Eigenschaften zusammengefasst, die verschiedene zugrunde liegende überprüfbare Datenstrukturen bieten können:

1. Inklusionsbeweis (Proof of Inclusion): Verifiziert, dass ein bestimmtes Element in der Datenstruktur enthalten ist.
2. Nicht-Inklusionsbeweis (Proof of Non-Inclusion): Verifiziert, dass ein bestimmtes Element nicht in der Datenstruktur enthalten ist.
3. Wertabruf für einen Schlüssel (Key Lookup): Ruft den (nachweisbaren und möglicherweise aktuellen) Wert ab, der einem gegebenen Schlüssel zugeordnet ist.
4. Append-only-Beweis (Proof of Append-Only): Stellt sicher, dass Daten nur angefügt, aber nicht verändert oder entfernt werden können.
5. Aufzählung der Einträge (Entries Enumeration): Erlaubt die Aufzählung aller Einträge in der Datenstruktur.
6. Beweis korrekter Ausführung (Proof of Correct Operation): Verifiziert, dass Operationen (etwa Zustandsübergänge) korrekt ausgeführt wurden.

7. Split-View-Erkennung (Split-View Detection): Ermöglicht Auditoren zu erkennen, ob verschiedenen Parteien inkonsistente Versionen der Datenstruktur gezeigt werden.

Zentrale Datenstrukturen in Transparenzsystemen

Um zu veranschaulichen, wie sich der Entwurf von Datenstrukturen auf die Effizienz der Beweise auswirkt, werden einige der am weitesten verbreiteten überprüfbaren Datenstrukturen und ihre wichtigsten Eigenschaften betrachtet:

Binäre Merkle-Hash-Bäume sind die zugrunde liegende überprüfbare Datenstruktur für Certificate Transparency. Es sind Binärbäume, in denen jeder Blattknoten den Hash eines Datenelements darstellt und jeder innere Knoten der Hash der Verkettung seiner Kindknoten ist. Merkle-Bäume liefern Inklusions- und Konsistenzbeweise. Diese Bäume sind auf logarithmische Beweiserzeugung und -verifikation optimiert, ihre Beweisgrößen können jedoch mit wachsender Eintragszahl unhandlich werden.

Sparse Merkle Trees (SMTs) erweitern das Merkle-Baum-Konzept auf große, möglicherweise dünn besetzte Datensätze, in denen viele Blätter leer oder nicht zugewiesen sein können. SMTs sind besonders nützlich in Key-Transparency-Systemen, in denen der Schlüsselraum groß, aber nur dünn besetzt ist. Diese Datenstruktur, auch Transparenz-Dictionary genannt, dient dazu, eine Menge von Schlüsseln (oder Labels) den entsprechenden Werten zuzuordnen. Dadurch lassen sich diese Bäume effizient nach einem bestimmten Wert abfragen. Bei Append-only-Logs gilt das nicht, da sie jedes Blatt iterativ durchlaufen müssen, bis die Daten gefunden sind. Außerdem erlauben SMTs einen effizienten Beweis der Abwesenheit eines Werts (auch Nicht-Mitgliedschaftsbeweise genannt), indem sie die als leer gekennzeichneten Blätter nutzen. Ein Append-only-Log wie das in CT verwendete muss dagegen den gesamten Baum neu berechnen, um einen solchen Nicht-Mitgliedschaftsbeweis zu erzeugen, da alle Blätter und ihre zugehörigen Inklusionsbeweise an die Auditoren übertragen werden müssen.

Kombination von Bäumen

Dieser hybride Ansatz kombiniert einen Präfixbaum für effiziente Schlüsselabfragen mit einem Verlaufsbaum (History Tree), der die chronologische Reihenfolge von Änderungen festhält. Solche Strukturen können sowohl effiziente Schlüssel-Wert-Abfragen als auch historische Abfragen unterstützen. Das macht sie vielseitig in Transparenzsystemen, in denen sowohl der aktuelle Zustand als auch historische Daten überprüft werden müssen. Diese Kombination ist besonders wirksam in Systemen wie Key Transparency, in denen sowohl der aktuelle Stand der Schlüssel als auch ihre historische Gültigkeit nachweisbar sein müssen.

Merkle Patricia Tries (MPTs)

Sie kombinieren einen Radix-Trie (oder Präfixbaum) mit einem Merkle-Baum, um Schlüssel-Wert-Speicheroperationen zu optimieren. Die Beweiserzeugung ist wegen der Trie-Struktur aufwendiger, doch dieser Aufwand lässt sich durch Optimierungen ausgleichen, die gemeinsame Präfixe in den Daten nutzen und die Gesamtgröße des Beweises verringern. Die Trie-Struktur ermöglicht platzsparendere Beweise, besonders bei Operationen mit Schlüsselpräfixen. Die Beweisverifikation bleibt effizient, kann aber wegen

des zusätzlichen Trie-Overheads rechenintensiver sein als bei Standard-Merkle-Bäumen. Merkle Patricia Tries eignen sich sehr gut für Anwendungen, in denen der Datensatz hierarchisch ist oder Präfixoperationen häufig vorkommen.

Merkle Forests

Merkle Forests sind Sammlungen von Merkle-Bäumen, die zur Verwaltung mehrerer unabhängiger Logs oder Datensätze dienen. Jeder Baum im Forest arbeitet unabhängig, kann aber mit einer gemeinsamen Wurzel oder einem aggregierten Beweis verknüpft werden. Merkle Forests erlauben parallele Beweiserzeugung, was die zur Erstellung von Beweisen benötigte Zeit in Systemen mit mehreren Logs deutlich verkürzen kann. Beweise aus verschiedenen Bäumen lassen sich aggregieren, sodass mehrere unabhängige Beweise zu einem einzigen überprüfbaren Beweis zusammengeführt werden können. Merkle Forests sind vorteilhaft in Multi-Tenant-Umgebungen, in denen verschiedene Benutzer oder Systeme getrennte Logs führen, aber einen einheitlichen Verifikationsmechanismus benötigen.

4.2. Bereinigungsmechanismen (Sanitization)

Der Bereinigungsmechanismus legt fest, wie Informationen in einem Log verwaltet werden, um Privatsphäre und Transparenz auszugleichen. Dieser Mechanismus bestimmt, ob Daten im Klartext (unbereinigt) oder mit verschiedenen datenschutzfreundlichen Techniken verarbeitet werden, die den Zugriff auf sensible Details einschränken. Zu den datenschutzfreundlichen Optionen zählen:

- Rauschen oder synthetische Daten: Daten können „bereinigt" werden, indem kontrolliertes Rauschen hinzugefügt oder synthetische Versionen erzeugt werden, die bestimmte Details verschleiern und statistische Eigenschaften erhalten. Dieser Ansatz ermöglicht die sichere Veröffentlichung von Daten, ohne Rohdaten preiszugeben.
- Verschlüsselung: In manchen Fällen werden protokollierte Daten verschlüsselt und nur bestimmten Parteien zugänglich gemacht, etwa vertrauenswürdigen Auditoren, die die Rohdaten entschlüsseln und prüfen können. Ebenso kann Einzelpersonen selektiver Zugriff auf Belege gewährt werden, die sie betreffen. Das wahrt die Privatsphäre und erlaubt gezielte Überprüfungen.
- Kryptografische Techniken: Fortgeschrittene Methoden wie Zero-Knowledge-Beweise erlauben die Überprüfung bestimmter Eigenschaften protokollierter Daten, ohne den eigentlichen Inhalt offenzulegen. Ein Zero-Knowledge-Beweis könnte beispielsweise bestätigen, dass bestimmte Ereignisse eingetreten sind oder dass Daten eine bestimmte Anforderung erfüllen, ohne die Daten selbst preiszugeben.

Gibt es keinen geeigneten Bereinigungsmechanismus, der die Transparenzanforderungen erfüllen kann, kann ein eingeschränkter Zugriff auf unbereinigte Daten notwendig sein. Lässt sich beispielsweise Differential Privacy nicht ohne übermäßiges Rauschen erreichen oder können kryptografische Beweise die nötigen Zusicherungen nicht vermitteln, kann bestimmten Auditoren Zugriff auf Rohdaten gewährt werden. Die Auditoren können dann geprüfte Berichte zur öffentlichen Kontrolle veröffentlichen, während die Allgemeinheit nur Zugriff auf eine bereinigte, datenschutzfreundliche Version der Daten hat, die die Ergebnisse der Prüfung widerspiegelt.

Zusätzlich können Kennungen oder Metadaten, mit denen Einzelpersonen ihre persönlichen Daten im Log überprüfen können, ebenfalls sorgfältig bereinigt werden müssen. Systeme wie CONIKS verwenden verifizierbare Zufallsfunktionen (Verifiable Random Functions, VRFs), um Benutzerkennungen zu erzeugen, die Identitäten verschleiern und dennoch Überprüfbarkeit ermöglichen. Neuere Ansätze [8] haben zudem Append-only-Zero-Knowledge-Sets eingeführt, die die durch Abfragen preisgegebenen Informationen begrenzen und so die Privatsphäre stärken, während sie Transparenz ermöglichen.

Durch solche Bereinigungsmechanismen können protokollierte Informationen Transparenz und Überprüfbarkeit bewahren und zugleich sensible Details schützen. Das unterstützt den Ausgleich zwischen Rechenschaftspflicht und individueller Privatsphäre.

4.3. Abfrage-, Überwachungs- und Prüfmechanismen

Transparenzsysteme setzen Abfrage-, Überwachungs- und Prüfmechanismen ein, damit Beteiligte den Inhalten des Systems vertrauen und Manipulationen oder unbefugte Handlungen erkennen können. Im Folgenden eine Aufschlüsselung dieser Mechanismen:

1. Abfragemechanismen

In Transparenzsystemen erlaubt das Abfragen (Querying) den Benutzern, das Vorhandensein und die Gültigkeit bestimmter Einträge zu prüfen. Certificate Transparency (CT) erlaubt es zum Beispiel jeder Person, Logs abzufragen, um das Vorhandensein eines Zertifikats zu überprüfen und sicherzustellen, dass es öffentlich protokolliert wurde und damit der Rechenschaftspflicht unterliegt. Key Transparency (KT) unterstützt den sicheren Lookup kryptografischer Schlüssel, die einem Benutzer zugeordnet sind, sodass Clients überprüfen können, ob sie für die sichere Kommunikation echte Schlüssel verwenden. Binary Transparency ermöglicht es Benutzern zu prüfen, ob eine bestimmte Software-Binärdatei verifiziert und protokolliert wurde, und trägt so zur Sicherung von Integrität und Echtheit bei.

Abfragemechanismen müssen effizient und datenschutzfreundlich gestaltet sein. Ihre Effizienz hängt stark von der zugrunde liegenden Datenstruktur ab (d. h. der Variante des Merkle-Baums), die es Benutzern erlaubt, Einträge zu überprüfen, ohne Zugriff auf den gesamten Log zu benötigen.

2. Überwachungsmechanismen

Überwachungssysteme (Monitoring) werden eingesetzt, um Inkonsistenzen, unbefugte Änderungen oder andere verdächtige Aktivitäten in Logs aktiv zu beobachten und zu erkennen. Log-Monitore sind unabhängige Dienste oder Werkzeuge, die Aktualisierungen von Logs in Echtzeit verfolgen und nach Unstimmigkeiten wie doppelten oder fehlenden Einträgen suchen. Sie können Benutzer oder Administratoren alarmieren, wenn mögliche Manipulationen oder Unregelmäßigkeiten festgestellt werden. In Systemen wie Certificate Transparency können Benutzer oder Drittdienste Zertifikats-Logs laufend überwachen und prüfen, ob eine Zertifizierungsstelle (Certificate Authority, CA) betrügerische Zertifikate ohne Wissen des Zertifikatsinhabers ausgestellt hat.

Überwachung ist in Transparenzsystemen wesentlich, um Bedrohungen schnell zu erkennen und zu beheben. Sie bietet zusätzliche Sicherheitsebenen über periodische Prüfungen hinaus.

3. Prüfmechanismen

Die Prüfung (Auditing) in Transparenzsystemen stellt sicher, dass Logs vertrauenswürdig bleiben und im Lauf der Zeit nicht verändert wurden. Sie wird typischerweise sowohl von den Benutzern des Systems als auch von externen Auditoren durchgeführt. Wichtige Aspekte sind:

- Konsistenzprüfungen: Auditoren verifizieren, dass Logs ihre Append-only-Eigenschaft bewahrt haben und nicht manipuliert oder neu geschrieben wurden. Das gelingt häufig durch Beweise, die die Konsistenz des Logs zu verschiedenen Zeitpunkten sicherstellen.
- Inklusions- und Konsistenzbeweise: Transparenzsysteme verwenden häufig kryptografische Beweise, um zu zeigen, dass ein Eintrag protokolliert wurde und mit früheren Einträgen konsistent bleibt. Diese Beweise sind besonders in Certificate Transparency und Key Transparency verbreitet, wo sie helfen zu überprüfen, dass Daten (z. B. Zertifikate, Schlüssel) korrekt protokolliert wurden.
- Audits durch Dritte: Transparenzsysteme laden häufig unabhängige Auditoren ein, den gesamten Log oder bestimmte Einträge regelmäßig zu überprüfen, was die Vertrauenswürdigkeit des Systems stärkt. In Key Transparency können Auditoren Dritter beispielsweise verifizieren, dass die öffentlichen Schlüssel der Benutzer korrekt protokolliert sind, sodass böswillige Akteure legitime Benutzer nicht imitieren können.

Durch diese Abfrage-, Überwachungs- und Prüfmechanismen helfen Transparenzsysteme, unbefugte Aktivitäten zu erkennen, Datenintegrität zu gewährleisten und überprüfbare Rechenschaftspflicht zu schaffen. Diese Mechanismen sind entscheidend für den Aufbau von Vertrauen, da sie unabhängige Überprüfung ermöglichen, die Privatsphäre wahren und sicheren, konsistenten Zugriff auf kritische Aufzeichnungen erlauben.

5. Prüfbarkeit der Nachweisphasen

Transparency Logs können den gesamten Lebenszyklus eines Nachweises (z. B. Ausstellung, Nutzung, Widerruf) aufzeichnen und unabhängige Beweise für jede ausgeführte Aktion liefern. Sie nutzen datenschutzfreundliche Methoden, um die Einhaltung von Datenschutzvorschriften sicherzustellen.

5.1. Ausstellung von Nachweisen

Die Ausstellung von Nachweisen ist der Prozess, in dem vertrauenswürdige Instanzen (Aussteller) überprüfbare Nachweise erstellen und an Benutzer verteilen. Die Nachweise selbst sind zwar kryptografisch signiert, doch zusätzliche Transparenz in diesem Prozess kann das Vertrauen weiter stärken. Benutzer müssen sicher sein, dass die erhaltenen Nachweise aus legitimen und vertrauenswürdigen Quellen stammen. Transparenz bei der Ausstellung stellt sicher, dass jeder erstellte Nachweis in einem öffentlichen oder verteilten Ledger protokolliert wird, sodass Benutzer die Identität des Ausstellers überprüfen und die Historie der Ausstellung nachverfolgen können. Transparenz hilft zu verhindern, dass böswillige oder gefälschte Aussteller betrügerische Nachweise erstellen. Ein transparenter Ausstellungs-Log würde solche Aktivitäten aufdecken, sodass Aussteller ihren Ruf wahren können und Prüfer den von Benutzern vorgelegten Nachweisen vertrauen. Schließlich können Ausstellungs-Logs eine prüfbare Spur darüber liefern, wann, wo und von wem Nachweise ausgestellt wurden. Das schafft Rechenschaftspflicht der Aussteller und stärkt das Gesamtvertrauen im Ökosystem.

5.2. Vorlage von Nachweisen

Wenn Benutzer ihre Nachweise mit Prüfern teilen (z. B. Arbeitgebern, Dienstanbietern), ist Transparenz im Vorlageprozess ebenso wichtig. Sie stellt sicher, dass sowohl der Benutzer als auch der Prüfer Vertrauen in die ausgetauschten Daten haben. Einer der wichtigsten Vorteile überprüfbarer Nachweise ist die Möglichkeit, nur die notwendigen Informationen zu teilen (z. B. nachzuweisen, dass man über 18 ist, ohne das vollständige Geburtsdatum offenzulegen). Transparenz bei der Vorlage von Nachweisen stellt sicher, dass nur die vereinbarten Daten weitergegeben wurden und nicht mehr [9]. Außerdem verifiziert Transparenz bei der Vorlage, dass der vorgelegte Nachweis nicht verändert wurde und der Benutzer der Weitergabe an den Prüfer zugestimmt hat. Durch eine transparente Spur stellt das System sicher, dass Benutzer die Kontrolle über ihre Daten behalten, und verifiziert zugleich, dass der Vorlageprozess gültig war.

5.3. Widerruf von Nachweisen

Der Widerruf von Nachweisen ist ein Mechanismus, der es Ausstellern erlaubt, einen zuvor ausgestellten Nachweis für ungültig zu erklären (z. B. wenn ein Führerschein entzogen wird oder eine berufliche Zertifizierung abläuft). Transparenz beim Widerruf stellt sicher, dass sowohl Benutzer als auch Prüfer den Status eines Nachweises leicht nachverfolgen können. Sie bietet eine klare Echtzeit-Methode, den Status jedes Nachweises zu überprüfen, und verhindert die Verwendung veralteter oder ungültiger Nachweise. Wurde ein Nachweis widerrufen (aufgrund eines Fehlers oder aus legitimem Grund), soll der Benutzer sofort informiert werden. Transparenz stellt sicher, dass Widerrufe öffentlich protokolliert werden und der Inhaber über jede Änderung seines Nachweisstatus Bescheid weiß. Außerdem müssen Prüfer sicher sein, dass der Nachweis, den sie akzeptieren, noch gültig ist. Ein transparentes Widerrufssystem erlaubt es ihnen, den aktuellen Status jedes Nachweises in Echtzeit zu prüfen und so sicherzustellen, dass sie nur gültige und vertrauenswürdige Informationen akzeptieren.

5.4. Wallet-Einrichtungsphase: Binary Transparency

Digitale Wallets sind der Eckpfeiler nutzerzentrierter Identitätsökosysteme, da sie überprüfbare Nachweise speichern und verwalten. Die Integrität der Wallet zu gewährleisten ist grundlegend, weil sie das wichtigste Werkzeug ist, auf das Benutzer bei der Verwaltung ihrer Nachweise angewiesen sind.

Binary Transparency bietet Vorteile wie:

- Schutz vor Manipulation und Schadsoftware: Binary Transparency stellt sicher, dass die vom Benutzer heruntergeladene Wallet-App nicht von böswilligen Akteuren manipuliert oder kompromittiert wurde. Benutzer können überprüfen, dass die Binärdatei dem ursprünglichen Quellcode entspricht, und haben so Vertrauen in die Funktionen der Wallet.

- Validierung bei Open Source: In manchen Fällen sind Wallets Open Source, sodass jede Person den Quellcode prüfen kann. Binary Transparency erlaubt es Benutzern sicherzustellen, dass die kompilierte Version der heruntergeladenen App dem von der Community geprüften ursprünglichen Code entspricht.

- Vertrauen in Updates: Regelmäßige Updates sind wesentlich, um Funktionalität und Sicherheit zu verbessern, können aber auch Risiken mit sich bringen. Binary-Transparency-Logs verifizieren, dass neue Releases von vertrauenswürdigen Entwicklern stammen und nicht verändert wurden, sodass die Sicherheit über die Zeit erhalten bleibt.

6. Entwurf eines Credential-Issuance-Transparency-Logs

6.1. CIT im Überblick

Dieser Abschnitt stellt Credential Issuance Transparency (CIT) [10] vor, einen datenschutzfreundlichen Audit-Logging-Mechanismus, der speziell für die Ausstellung identifizierender Nachweise entworfen wurde. CIT baut auf dem Konzept von Append-only-Logs auf, wie sie bei Certificate Transparency (CT) zu finden sind, passt es aber an, um sensible Informationen zu schützen. Indem Log-Einträge vollständig geblindet werden, entfernt CIT alle identifizierenden Angaben. So bleibt die Privatsphäre der Benutzer gewahrt, die öffentliche Prüfbarkeit der Append-only-Struktur des Logs bleibt erhalten, und Einzelpersonen können Nachweise überprüfen, die sie betreffen.

Anstatt einen öffentlich sichtbaren Domainnamen oder andere identifizierende Informationen anzuzeigen, verwendet CIT ein zufällig geblindetes Commitment, um die Identität des Nachweisinhabers zu verbergen. Das stellt sicher, dass nur berechtigte Parteien einen Nachweis mit seinem Inhaber verknüpfen können, während die Öffentlichkeit weiterhin validieren kann, dass die Ausstellung des Nachweises ordnungsgemäß protokolliert wurde.

CIT übernimmt außerdem das Vertrauensmodell von CT und stützt sich auf vertrauenswürdige Prüfer, die Protokollierungspflichten durchsetzen. Um als gültig akzeptiert zu werden, muss jeder Nachweis einen entsprechenden Eintrag im CIT-Log haben, sodass alle Ausstellungen von Nachweisen ordnungsgemäß erfasst sind. Die geblindete Natur dieser Log-Einträge führt jedoch eine zusätzliche Validierungsherausforderung ein: die Echtheit eines Nachweises zu überprüfen, ohne sensible Informationen preiszugeben. Dazu setzt CIT nicht-interaktive Zero-Knowledge-Beweise (NIZKPs) ein. Diese Beweise erlauben es dem Aussteller des Nachweises, zu belegen, dass ein Log-Eintrag mit dem zugehörigen Nachweis konsistent ist, ohne private Daten offenzulegen.

Wie in Abbildung 3 dargestellt, ermöglicht CIT Benutzern, die Ausstellung aller identifizierenden Nachweise zu überwachen, die möglicherweise dazu verwendet werden könnten, sie zu imitieren. Indem CIT einen sicheren, datenschutzfreundlichen Rahmen für die Ausstellung von Nachweisen bietet, unterstützt es die Prinzipien der Self-Sovereign Identity und nähert sich einem Modell, das für Gesetzgeber und Regulierungsbehörden akzeptabel ist.

Dieser Audit- und Logging-Ansatz fördert Rechenschaftspflicht und schützt zugleich die Privatsphäre. Er überbrückt die Lücke zwischen Transparenz und individueller Sicherheit in Frameworks für digitale Identität. Damit deckt CIT einen kritischen Bedarf an überprüfbarer, datenschutzzentrierter Prüfbarkeit ab, die für den Aufbau von Vertrauen in Self-Sovereign-Identity-Systeme und die breitere Einführung im öffentlichen wie im privaten Sektor wesentlich ist.

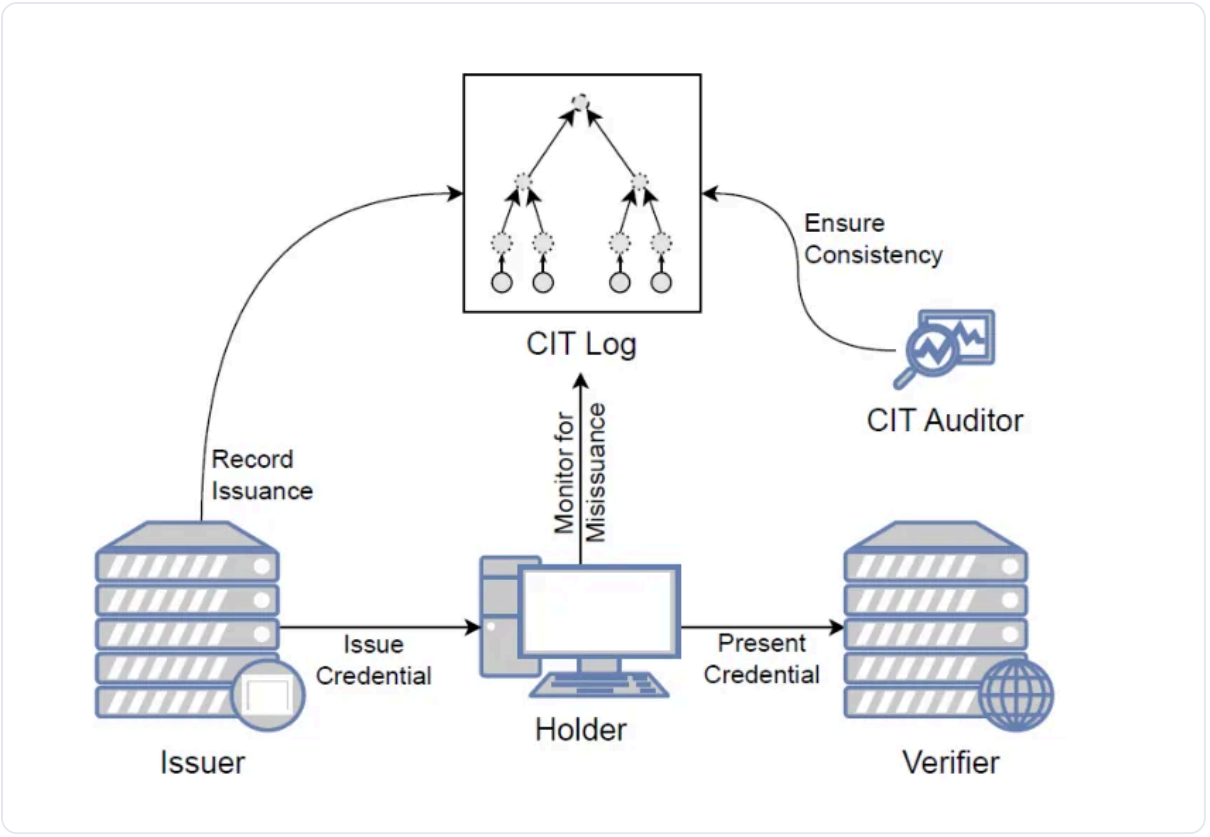


Abbildung 3: CIT im Überblick

6.2. Protokolle

Um diese Herausforderungen anzugehen, wird das Protokoll Credential Issuance Transparency (CIT) vorgeschlagen, ein datenschutzfreundlicher Rahmen zur Prüfung der Ausstellung von Nachweisen. Dieses Protokoll soll sicherstellen, dass identifizierende Nachweise sicher und überprüfbar protokolliert werden, ohne sensible Benutzerinformationen offenzulegen. So können Benutzer und Prüfer gleichermaßen die Ausstellung von Nachweisen datenschutzbewusst bestätigen.

In CIT besteht jeder Log-Eintrag aus zwei Hauptelementen: dem Hash-Digest des Nachweises selbst und einem geblindeten Commitment, das an die eindeutige Kennung des Benutzers (UserID) gebunden ist. Dieser Ansatz stellt sicher, dass keine sensiblen Details offengelegt werden, während das Commitment es Benutzern ermöglicht, für sie relevante Log-Einträge zu identifizieren und zu überprüfen. Kennen Benutzer ihre UserID, können sie einfach eine Probeberechnung durchführen, um festzustellen, ob ein bestimmter Log-Eintrag zu ihrem Nachweis gehört. Das stärkt die Transparenz, ohne die Privatsphäre zu beeinträchtigen.

Damit Prüfer die Log-Einträge authentifizieren können, ohne Zugriff auf sensible Benutzerdaten zu erhalten, setzt CIT einen nicht-interaktiven Zero-Knowledge-Pre-Image-Beweis ein. Dieser kryptografische Beweis erlaubt es Prüfern zu bestätigen, dass das geblindete Commitment in einem gegebenen Log-Eintrag zur UserID gehört, die dem Pseudonym eines Benutzers zugrunde liegt, ohne die eigentliche UserID preiszugeben. Dadurch können Prüfer die Legitimität der Ausstellung des Nachweises feststellen, ohne Zugriff auf personenbezogene Daten zu erhalten. Tabelle 1 fasst die von CIT eingeführten Protokolle ausführlicher zusammen.

Das CIT-Protokoll schafft somit einen Ausgleich zwischen Prüfbarkeit und Privatsphäre. Es ermöglicht Benutzern, ihre Nachweise auf unbefugte Ausstellung zu überwachen, und erlaubt Prüfern, die Gültigkeit von Nachweisen zu bestätigen. Indem CIT einen sicheren, datenschutzfreundlichen Mechanismus für das Audit-Logging von Nachweisen bietet, unterstützt es ein transparentes, überprüfbares System, das mit datenschutzorientierten Prinzipien im Einklang steht, und ist damit ein wertvoller Baustein in sicheren Ökosystemen für digitale Identität. Diese Innovation ebnet den Weg für robustere Self-Sovereign-Identity-Frameworks, in denen Privatsphäre und Transparenz harmonisch verbunden sind, um Vertrauen und Compliance im Management digitaler Identitäten zu stärken.

Protokoll zur Ausstellung von Nachweisen:

1. Aussteller stellt Nachweis aus: x basierend auf $UserId$
2. CIT fügt Log-Eintrag an: l : = (n, $C(n, UserId)$, $H(x)$)
3. CIT gibt signierten Inklusionsbeweis zurück
4. Aussteller fügt l und Inklusionsbeweis an x an und gibt ihn an den Benutzer zurück

Protokoll zur Vorlage von Nachweisen:

1. Benutzer zeigt dem Prüfer x, l und Inklusionsbeweis
2. Prüfer erfährt p : = $P(s, userId)$
3. Benutzer liefert NIZKP für $C(n, UserId) \wedge p = P(s, UserId)$
4. Prüfer prüft $H(x)$ und NIZKP, um die korrekte Protokollierung sicherzustellen

Entdeckungsprotokoll (Discovery):

1. Benutzer fordert alle neuen Audit-Log-Einträge an
2. Für jeden Eintrag (n, $C(n, UserID')$, $H(x)$) berechnet der Benutzer probeweise $C(n, UserID)$ == $C(n, UserID')$
    - a. Benutzer vergleicht H(x) mit seinen Nachweisen
    - b. Wird keine Übereinstimmung gefunden, hat der Benutzer einen fehlerhaft ausgestellten Nachweis erkannt

Tabelle 1 CIT-Protokolle für Ausstellung, Vorlage und Entdeckung

6.3. Leistungsbewertung

Es wird analysiert, wie praktikabel der Einsatz von Credential Issuance Transparency (CIT) in realen Umgebungen ist. Die Analyse kommt zu dem Schluss, dass er machbar ist. Im Folgenden eine Zusammenfassung der wichtigsten Leistungsaspekte:

Log-Größe und Download-Anforderungen: In CIT müssen Benutzer (in der Rolle von Monitoren) neue Log-Einträge herunterladen, die seit ihrer letzten Prüfung angefügt wurden. Zum Vergleich: In Certificate Transparency (CT) im Web-PKI-System ergeben eine durchschnittliche Log-Eintragsgröße von 5,93 KB und ein tägliches Wachstum von etwa 7,8 Millionen Einträgen 43,99 GB neue Log-Daten pro Tag. Das ist ein Umfang, den nur große Organisationen bewältigen können. CIT dagegen verwendet vollständig geblindete Daten, was zu einer konstanten Log-Eintragsgröße von nur 96 Byte führt. Selbst bei der hohen Wachstumsrate von CT würden dadurch nur 746 MB neue Daten pro Tag entstehen, was für Einzelpersonen mit einer üblichen Internetverbindung zu Hause zu bewältigen ist.

Verifikationsberechnung: Nach dem Herunterladen der Einträge müssen Benutzer Probe-Hashes berechnen, um ihre UserID-Commitments zu vergleichen. Mit SHA-256 erreicht moderne Consumer-Hardware mit Hash-Beschleunigung mehr als 3 Millionen Hashes pro Sekunde. Benutzer könnten somit die in CT-Studien berichteten 8 Millionen täglichen Einträge selbst unter Berücksichtigung des Systemoverheads problemlos bewältigen.

Einreichung von Log-Einträgen und Append-Beweise: Jede Einreichung eines Eintrags erfordert einen Append-Beweis, der nur minimale Datenübertragung verursacht. Die Größe des Merkle-Tree-Append-Beweises wächst logarithmisch mit der Anzahl der Einträge. Unter der Annahme von SHA-256-Hashes und täglichen Eintragsraten ähnlich wie bei CT bleibt die Beweisgröße unter 1 KB pro Eintrag, was hinsichtlich der Bandbreite unerheblich ist.

Insgesamt bleiben die Überwachungsanforderungen von CIT selbst bei einer globalen Verbreitung in der Größenordnung von CT für Einzelpersonen auf üblichen Heim-PCs machbar. Außerdem verursachen die Logging-Operationen von CIT bei der Ausstellung von Nachweisen keinen spürbaren Mehraufwand, was einen breiten Einsatz praktikabel macht.

Beweise der Logging-Korrektheit: Die Implementierung des Zero-Knowledge-Beweises (ZKP) wurde auf einem Intel-i7-8550U-Laptop gemessen. Tabelle 1 zeigt die Ergebnisse, Abbildung 3 bietet eine Visualisierung. Der Prozess gliedert sich in drei Phasen:

1. Initiierungsphase: Wird einmal für das gesamte System durchgeführt, einschließlich Trusted Setup und Schaltkreiskompilierung.
2. Vorbereitungsphase: Wird einmal pro Nonce-userID-spID-Tupel ausgeführt, was Benutzer vorab berechnen können.
3. Vorzeigephase: Wird vom Prüfer jedes Mal durchgeführt, wenn ein Nachweis vorgezeigt wird. Diese Phase ist schnell genug, dass Caching beim Prüfer in der Regel nicht nötig, aber möglich ist.

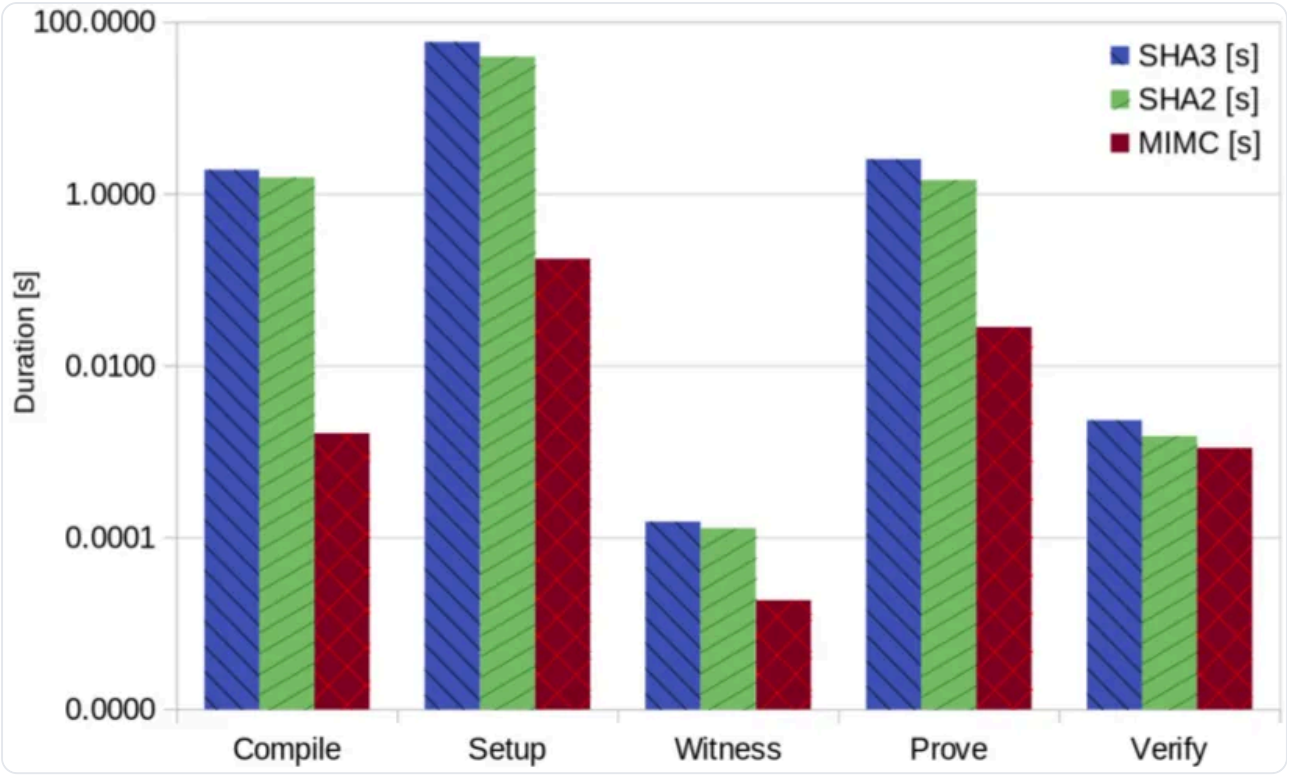


Abbildung 4: NIZKP-Auswertung Tabelle 1 Auswertungsergebnisse

		BN254		
		MiMC	SHA256	SHA3-256
	security		102 bit	
	#constraints	1322	170157	235032
initiation	compile policy [s]	0.002	1.541	1.891
	setup (gen. keys) [s]	0.176	39.134	58.189
prepare	gen. witness [s]	0.00002	0.0001	0.0002
	prove statement [s]	0.028	1.444	2.515
show	verify proof [s]	0.001	0.002	0.002

Abbildung 4: vergleicht die Leistung verschiedener Hashfunktionen für jede Phase des NIZKP-Beweises. Tabelle 2 enthält die für jede der Phasen erzielten Auswertungsergebnisse.

Diese Ergebnisse zeigen, dass die ZKP-Implementierung effizient ist, besonders in der Vorzeigephase, und sich damit für Echtzeit-Verifikation eignet.

Insgesamt zeigen die Auswertungen, dass CIT hochgradig praktikabel ist und die Systemleistung nur minimal beeinflusst. Bei der Vorlage von Nachweisen fügt CIT einen Overhead von weniger als 2 Millisekunden hinzu, der in Echtzeitanwendungen praktisch nicht wahrnehmbar ist. Außerdem müssen Benutzer, die auf unbefugte Ausstellung von Nachweisen achten wollen, nur etwa 1 GB Daten pro Tag herunterladen, was für die meisten Internetverbindungen zu bewältigen ist. Der Verifikationsprozess ist ebenso effizient und erfordert weniger als 10 Sekunden Rechenaufwand. Diese geringen Ressourcenanforderungen machen CIT zu einer praktikablen Lösung für eine breite Einführung, auch für Einzelpersonen auf üblichen Geräten.

7. Schlussfolgerungen:

Dieses Projekt wollte zeigen, dass Transparency Enhancing Technologies (TETs), insbesondere protokollbasierte Transparency Logs, eine entscheidende Rolle dabei spielen, dass digitale Identitäten und überprüfbare Nachweise unabhängig geprüft und verifiziert werden können. Es schafft einen offenen und überprüfbaren Rahmen, in dem Benutzer, Aussteller und Prüfer sicher und mit Zuversicht interagieren können. Durch die Integration von Transparenz in jede Phase, also Wallet-Binärdateien, Ausstellung, Vorlage und Widerruf von Nachweisen, können Ökosysteme für digitale Identität mehrere zentrale Ziele erreichen:

- Mehr Rechenschaftspflicht: Alle Akteure, einschließlich Aussteller und Wallet-Entwickler, sind durch prüfbare und überprüfbare Logs für ihre Handlungen rechenschaftspflichtig.
- Höhere Sicherheit: Transparenz fügt Sicherheitsebenen hinzu, verhindert Manipulation, Betrug und Missbrauch von Nachweisen und stellt sicher, dass Daten sicher und geschützt bleiben.
- Stärkung der Benutzer: Durch Einblick in die Systeme und Prozesse sind Benutzer in der Lage, fundierte Entscheidungen darüber zu treffen, wie sie ihre Identitäten verwalten und teilen.

Außerdem wurde Credential Issuance Transparency (CIT) vorgestellt, ein Framework, das Transparenz und Vertrauen bei der Ausstellung identifizierender Nachweise in digitalen Identitätssystemen stärken soll. CIT ermöglicht Benutzern, die Ausstellung ihrer Nachweise zu überwachen, sodass fehlerhafte oder unbefugte Ausstellung schnell erkannt und geprüft werden kann. Wichtig ist, dass CIT dies bei gleichbleibender Effizienz und Benutzbarkeit erreicht: Es fügt bei der Vorlage von Nachweisen einen nicht wahrnehmbaren Overhead von weniger als 2 Millisekunden hinzu, erfordert für die Überwachung nur minimale tägliche Downloads von unter 1 GB und schließt die rechnerische Verifikation in weniger als 10 Sekunden ab.

Diese Eigenschaften machen CIT zu einer praktikablen Lösung für den Einsatz in der Praxis. Sie unterstützt sichere und datenschutzfreundliche Prüfbarkeit, ohne Benutzer oder Systeme zu belasten. Da digitale Identität für sichere Online-Interaktionen zunehmend zentral wird, bietet CIT einen grundlegenden Schritt hin zu einem rechenschaftspflichtigen, überprüfbaren Management von Nachweisen, das mit Datenschutzprinzipien im Einklang steht. Dieses Framework hat somit das Potenzial, mehr Vertrauen in Ökosysteme für digitale Nachweise zu schaffen und die Verbreitung selbstbestimmter und nutzerzentrierter Identitätsmodelle voranzubringen.

Literaturverzeichnis

[1] “EU Digital Identity Wallet Home - EU Digital Identity Wallet -.” Accessed: Nov. 11, 2024. [Online]. Available: https://ec.europa.eu/digital-buildingblocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home

[2] “The European Digital Identity Regulation (eIDAS 2): Framework and Insights.” Accessed: Nov. 11, 2024. [Online]. Available: https://www.european-digital-identity-regulation.com/

[3] A. Hicks, “SoK: Log Based Transparency Enhancing Technologies,” May 2023, Accessed: Nov. 11, 2024. [Online]. Available: http://arxiv.org/abs/2305.01378

[4] “Certificate Transparency : Certificate Transparency.” Accessed: Nov. 11, 2024. [Online]. Available: https://certificate.transparency.dev/

[5] “Verifiable Credentials Data Model v2.0.” Accessed: Apr. 02, 2024. [Online]. Available: https://www.w3.org/TR/vc-data-model-2.0/

[6] “Deploying key transparency at WhatsApp - Engineering at Meta.” Accessed: Nov. 11, 2024. [Online]. Available: https://engineering.fb.com/2023/04/13/security/whatsapp-keytransparency/

[7] “What are zk-SNARKs? - Z.Cash.” Accessed: Nov. 11, 2024. [Online]. Available: https://z.cash/learn/what-are-zk-snarks/

[8] M. Chase, E. Ghosh, A. Deshpande, and H. Malvai, “Seemless: Secure end-to-end encrypted messaging with less trust,” *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 1639–1656, Nov. 2019, doi: 10.1145/3319535.3363202/SUPPL_FILE/P1639-MALVAI.WEBM.

[9] S. More, J. Heher, E. Fasllija, and M. Mathie, “Service Provider Accreditation: Enabling and Enforcing Privacy-by-Design in Credential-based Authentication Systems,” *ACM International Conference Proceeding Series*, p. 86, Jul. 2024, doi: 10.1145/3664476.3669934.

[10] E. Fasllija, J. Heher, and S. More, “Credential Issuance Transparency: A Privacy-preserving Audit Log of Credential Issuance,” Sep. 04, 2024, *Springer* . Accessed: Nov. 11, 2024. [Online]. Available: https://graz.elsevierpure.com/en/publications/credential-issuance-transparency-aprivacy-preserving-audit-log-o