Fraunhofer SIT

Datensparsame Altersverifikation

Konzeptbeschreibung

Juli 2024

1 Einleitung

Das vorliegende Dokument beschreibt das Konzept für ein Protokoll, mit dessen Hilfe ein datensparsamer Nachweis über die Zugehörigkeit einer Person zu einer Altersgruppe (Alterskohorte) gegenüber einem Anbieter von Diensten im Internet erbracht werden kann. Dabei vermittelt ein Nutzer des Protokolls zwischen einem Anbieter und einer weiteren Stelle, die die Zugehörigkeit des Nutzers zu einer Alterskohorte verifizieren kann. Das Protokoll soll es ermöglichen, in einem geeigneten und kooperativen Umfeld eine Altersverifikation durchzuführen und dabei nur ein Minimum an notwendigen Daten an die beteiligten Kommunikationspartner zu übermitteln. Der Diensteanbieter soll nur eine Zugehörigkeit zu einer Alterskohorte, aber keine weiteren Informationen über den Nutzer erhalten. Die Stelle, die die Zugehörigkeit des Nutzers zur Alterskohorte verifiziert, soll nicht erfahren, für welchen Anbieter und welche Art von Dienst der Nutzer einen Altersnachweis benötigt.

Für das Konzept wird eine möglichst hohe Kompatibilität und Interoperabilität zu existierenden Technologien angestrebt. Insbesondere können die Parteien, die die Altersverifikation durchführen, sehr unterschiedlich gestaltet sein, was ihre jeweilige Methode zur Feststellung des Alters betrifft. Notwendig ist für verifizierende Parteien (»Verifizierer«) ausschließlich die Umsetzung der entsprechenden Schnittstellen zum beschriebenen Protokoll und eine Aufnahme in die Gruppe von vertrauenswürdigen Instanzen zur Altersverifikation durch eine geeignete übergeordnete Stelle (»Zertifizierungsstelle«).

1.1 Umfeld

Altersverifikation und ähnliche Methoden wie Altersschätzungen werden im Kontext des Jugendschutzes vielfältig erörtert. Ein häufig diskutierter Punkt ist der Zugang Minderjähriger zu Pornografie [2]. Dabei zeigt sich immer wieder, wie schwierig eine Umsetzung einer Zugangsbeschränkung ist [6, 17]. Dabei spielt auch die Art, wie für entsprechende Inhalte geworben wird eine Rolle [10], was wiederum den Kontakt erleichtert [8]. Aber auch andere Fragestellungen wie der Versand von Alkohol an Minderjährige werden erörtert [1]. Nash *et al.* zählen in ihrer Studie im Kontext von Online-Glücksspiel zur Alterskontrolle unter anderem technische Ansätze und Initiativen [16]. Auch der Versand von Zigaretten und Cannabidiol wird thematisiert [20, 4].

Die Entwicklung von Lösungen ist dabei nicht trivial. In seinem Aufsatz betont Tobias Keber, dass die komplexe Beziehung zwischen Datenschutzrecht und den

Freiheiten der Medien- und Informationsverbreitung, wie beim Medienprivileg, oft unausgewogen diskutiert wird [11]. Insbesondere weist er darauf hin, dass der Datenschutz bei der Bewertung von Jugendschutzmaßnahmen, wie bei TikTok, vernachlässigt wird. Es ist entscheidend, Datenschutz und Jugendschutz gemeinsam zu betrachten, da Datenschutz auch ein wesentlicher Bestandteil des Jugendschutzes ist.

Kinder und Jugendliche haben das Recht[1] auf Zugang zu Informationen und die Teilhabe an der digitalen Welt [19], was für ihre Bildung und soziale Entwicklung von wesentlicher Bedeutung ist. Dieses Recht steht jedoch in einem Spannungsverhältnis zum notwendigen Schutz vor unangemessenen Diensten im Internet [18]. Eltern besitzen wiederum das Recht und die Pflicht, die Internetnutzung ihrer Kinder dahingehend zu regulieren und zu begrenzen, dass Schutz und Sicherheit der Kinder gewährleistet sind, also beispielsweise auch sichergestellt ist, dass ihre Kinder nur Zugang zu altersgerechten Diensten erhalten. Dazu können Maßnahmen wie die Implementierung von Kindersicherungen auf digitalen Geräten oder die Anpassung von Datenschutzeinstellungen bei verschiedenen digitalen Diensten eingesetzt werden. Auch technische Maßnahmen wie Altersverifikationssysteme können dabei eine wesentliche Rolle spielen.

Lösungen zur Altersverifikation, die einen starken Fokus auf Datenschutz legen, schützen die Privatsphäre von Kindern und Jugendlichen und verhindern den Missbrauch personenbezogener Daten. Sie leisten somit einen Beitrag dazu, dass auch Kinder und Jugendliche ihr Recht auf Informations- und Meinungsfreiheit in vollem Umfang wahrnehmen können, ohne sich zusätzlichen Risiken beispielsweise durch Überwachung oder Datenmissbrauch auszusetzen. Eine Minimierung der personenbezogenen Daten, die bei geeigneten Lösungen zur Altersverifikation benötigt werden, stärkt das Recht auf eine anonyme und pseudonyme Nutzung von Diensten sowohl für Erwachsene als auch für Minderjährige: Anbieter können ihre Dienste sicher für verschiedene Altersgruppen zur Verfügung stellen, ohne auf die Speicherung von zusätzlichen personenbezogene Daten angewiesen zu sein.

1.2 Abgrenzung

Um das vorgestellte Konzept korrekt einordnen zu können, sind einige Abgrenzungen notwendig. Die eigentlichen Ansätze zur Feststellung des Alters einer Person werden hier nicht behandelt – sie bilden über Verifizierer eine abstrakte Instanz, die im Rahmen des Konzepts nur die Aufgabe hat, über eine vordefinierte Schnittstelle signierte Bestätigungen zu erzeugen (»Altersnachweise«). Für die Umsetzung des Konzepts ist es notwendig, dass eine oder mehrere solcher Instanzen existieren.

Datensparsamkeit kann insbesondere dann erreicht werden, wenn ein Anbieter keine personenbezogenen Daten über einen Nutzer erfordert. Hier kann, wenn

[1] https://www.kinderrechte.de/kinderrechte/un-kinderrechtskonvention-im-wortlaut#c3252

vom Nutzer gewünscht, bereits eine einfache Kontaktmöglichkeit (etwa eine pseudonyme oder anonyme E-Mail-Adresse ohne Personenbezug) in Kombination mit dem vorgestellten Konzept eine längerfristige, personengebundene Nutzung des Anbieters ermöglichen, bei der eine minimale Menge an Daten gegenüber dem Anbieter preisgegeben wird. Auch ist unter Verwendung des Konzepts eine langfristige anonyme Nutzung von Anbietern möglich (sofern diese für ihre Dienste kein Nutzerkonto erfordern), da für die Durchführung der datensparsamen Altersverifikation selbst kein Nutzerkonto bei einem Anbieter erforderlich ist.

Das im Konzept definierte Protokoll kann die Durchsetzung einer Altersverifikation bei Anbietern nicht erzwingen. Es ist notwendig, dass Anbieter ein Eigeninteresse an einer nachvollziehbaren Altersverifikation entwickeln und entsprechende Mechanismen einsetzen möchten, um den Zugriff auf altersbeschränkte Dienste verantwortungsvoll zu gestalten. Illegale Angebote oder solche aus Ländern, die Vorgaben zum Jugendschutz nicht umsetzen, können mit diesem Konzept nicht unterdrückt werden.

Wichtig ist auch, zwischen dem Konzept und seiner Umsetzung zu differenzieren. In diesem Dokument wird ein Konzept vorgestellt und anhand einer beispielhaften Umsetzung als Browser-Extension für Demonstrationszwecke implementiert. Dasselbe Konzept kann aber ebenso auf anderen Wegen umgesetzt werden, wie auch in Kapitel 4 diskutiert wird.

1.3 Aufbau

Im nachfolgenden Kapitel 2 werden die Grundlagen des Konzepts beschrieben, wobei zunächst verschiedene bekannte Verfahren zur Altersverifikation aufgeführt, aber auch die wesentlichen Elemente des Konzepts eingeführt werden. In Kapitel 3 wird das Konzept vorgestellt. Danach werden in Kapitel 4 praktische Umsetzungsmöglichkeiten diskutiert und in Kapitel 5 Herausforderungen bei der Umsetzung des Konzepts erörtert.

2 Grundlagen der Altersverifikation

In diesem Kapitel werden verschiedene Grundlagen, Technologien und Abläufe zur Durchführung einer Altersverifikation vorgestellt. Einige der aufgeführten existierenden Verfahren zur Altersverifikation können bei einer praktischen Umsetzung des vorgestellten Konzepts von Verifizierern eingesetzt werden, wenn sie mit den entsprechenden Schnittstellen ausgestattet werden.

In den technischen Grundlagen werden Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität) sowie digitale Signaturen, Public-Key-Infrastrukturen und abstrakte kryptografische Primitive und Protokolle vorgestellt, um eine Terminologie für das Konzept einzuführen. Zuletzt wird in diesem Kapitel der Begriff der Datensparsamkeit erläutert, die einen zentralen Aspekt des vorgestellten Konzepts zur Altersverifikation darstellt.

2.1 Altersverifikationsverfahren in Deutschland

In Deutschland gibt es verschiedene Methoden zur Altersverifikation, um sicherzustellen, dass Minderjährige keinen Zugang zu altersbeschränkten Inhalten oder Diensten erhalten. Diese Methoden werden sowohl online als auch offline angewendet und müssen den Datenschutz- und Jugendschutzgesetzen entsprechen. Gängige Methoden sind:

Post-Ident-Verfahren Das Post-Ident-Verfahren wird von der Deutschen Post angeboten. Dabei wird die Identität des Nutzers in einer Postfiliale überprüft. Der Nutzer muss dort einen gültigen Ausweis vorlegen, und die Post bestätigt dann die Identität und das Alter des Nutzers gegenüber dem Dienstanbieter [3].

Video-Ident-Verfahren Beim Video-Ident-Verfahren erfolgt die Verifikation per Videoanruf. Der Nutzer zeigt einem Mitarbeiter eines zertifizierten Anbieters seinen Ausweis über eine Webcam. Der Mitarbeiter prüft die Echtheit des Ausweises und die Übereinstimmung mit der Person, die ihn vorlegt [12, 15].

Schufa-Identitäts-Check Dieser Dienst überprüft das Alter und die Identität des Nutzers durch einen Abgleich mit der Datenbank der Schufa. Der Nutzer gibt dazu seine Daten online ein und die Schufa bestätigt dem Anbieter das Alter und die Identität [13].

Personalausweis mit Online-Ausweisfunktion Mit dem Personalausweis und der Online-Ausweisfunktion kann das Alter online verifiziert werden [14]. Der Nutzer benötigt dafür einen NFC-fähigen Kartenleser oder ein NFC-fähiges Smartphone sowie die entsprechende AusweisApp.

Kreditkarten-Verifizierung Da in Deutschland nur Personen ab 18 Jahren eine eigene Kreditkarte besitzen dürfen, wird manchmal eine Kreditkarte zur Altersverifikation verwendet. Dabei wird eine kleine Testabbuchung vorgenommen, um sicherzustellen, dass die Karte gültig und auf den Nutzer registriert ist. Entsprechende Verfahren existieren auch für Girokarten.

Altersprüfung über Einwohnermeldeamt Einige Dienste bieten an, das Alter über eine Abfrage beim Einwohnermeldeamt zu verifizieren. Hierbei wird die Erlaubnis des Nutzers eingeholt, damit der Dienstanbieter eine Altersbestätigung direkt vom Meldeamt erhält [7].

Jugendschutzprogramme Einige Anbieter nutzen spezielle Jugendschutzprogramme, die von der Kommission für Jugendmedienschutz (KJM)[1] anerkannt sind. Diese Programme kombinieren verschiedene Aspekte wie technische Maßnahmen und persönliche Identitätsnachweise, um sicherzustellen, dass nur berechtigte Nutzer Zugriff auf bestimmte Inhalte erhalten.

[1] https://www.kjm-online.de/themen/technischer-jugendmedienschutz

2.2 Technische Grundlagen

Die Überprüfung des Alters eines Nutzers ist ein kritischer Prozess, in dem nicht nur sichergestellt werden muss, dass die angegebenen Daten korrekt sind, sondern auch, dass diese Daten authentisch und vor Manipulationen geschützt sind. Nachfolgend werden Schutzziele wie Vertraulichkeit oder Authentizität sowie technische Grundlagen wie digitale Signaturen beschrieben, die für das vorgestellte Konzept essenziell sind.

Vertraulichkeit Der Schutz vor unbefugtem Zugriff auf Informationen bzw. Daten wird als Vertraulichkeit bezeichnet und stellt ein wichtiges Ziel der Informationssicherheit dar. Vertraulichkeit wird in IT-Systemen typischerweise durch den Einsatz von Verschlüsselung erreicht, die zur Speicherung und Übertragung von Daten eingesetzt wird und sicherstellt, das nur befugte Personen Zugriff auf diese Daten bekommen.

Integrität Ein weiteres Schutzziel der Informationssicherheit ist die Integrität, womit die Unversehrtheit eines IT-Systems oder von Daten innerhalb eines IT-System bezeichnet wird. Eine Gewährleistung von Integrität bedeutet, dass sichergestellt werden kann, dass Daten innerhalb eines IT-Systems nicht unbemerkt verändert werden können, weder durch fehlerhafte Datenverarbeitungsprozesse oder defekte Datenspeicher noch durch Angreifer mit Manipulationsabsichten. Mechanismen, die zur Datenintegrität beitragen, sind beispielsweise Prüfsummen (kryptografische Hashes), die von beliebigen Daten berechnet werden können und anhand derer schnell feststellbar ist, ob Daten verändert wurden.

Verfügbarkeit Verfügbarkeit bezeichnet das Schutzziel, die Ausfallsicherheit eines IT-Systems und damit verbunden den Zugriff auf seine Dienste und Daten innerhalb eines definierten Zeitraums zu gewährleisten. In komplexeren IT-Architekturen, die aus verschiedenen IT-Systemen bestehen, kann die Verfügbarkeit der gesamten Architektur ggf. von wenigen kritischen IT-Systemen abhängen, die für die Funktionsfähigkeit der Architektur notwendig sind.

Authentizität Authentizität bezieht sich in der Informatik auf die Eigenschaft, dass die Herkunft und der Inhalt von Daten als echt und unverändert bestätigt werden können. Authentizität ist ein zentraler Aspekt der Informationssicherheit und spielt eine wesentliche Rolle in der Vertrauenswürdigkeit von Systemen und Kommunikationsprozessen. Die Authentizität der bereitgestellten Altersinformationen ist von grundlegender Bedeutung. Diese kann durch verschiedene Mechanismen sichergestellt werden, darunter der Einsatz von verlässlichen Identitätsnachweisen und biometrischen Verifikationsmethoden.

Digitale Signaturen Bei der Sicherstellung der Authentizität und Integrität von Daten innerhalb digitaler Kommunikationssysteme spielen digitale Signaturen eine wichtige Rolle. Eine digitale Signatur ist eine kryptografische Technik, die es ermöglicht, die Authentizität und Integrität einer Nachricht oder eines Dokuments zu verifizieren. In einem Protokoll zur Altersverifikation kann eine digitale Signatur verwendet werden, um zu bestätigen, dass eine Information über das Alter einer Person von einer vertrauenswürdigen Quelle stammt und das diese Information seit der Signatur nicht verändert wurde. Dies wird durch den Einsatz asymmetrischer Kryptografie erreicht, bei der ein öffentlicher und ein privater Schlüssel verwendet werden. Der private Schlüssel, der vertraulich behandelt wird, wird zur Signatur einer Nachricht verwendet, während der öffentliche Schlüssel, der allgemein zugänglich ist, zur Überprüfung der Signatur verwendet wird.

Public-Key-Infrastruktur (PKI) Eine PKI ist ein System oder ein Framework, das digitale Zertifikate ausstellen, verteilen und überprüfen kann, die zur sicheren Kommunikation zwischen verschiedenen Parteien eingesetzt werden können. Digitale Zertifikate werden hierbei von einer oder mehreren vertrauenswürdigen Zertifizierungsstellen ausgegeben und dienen zur Identifikation von Teilnehmern innerhalb der PKI und zur Prüfung von Signaturen dieser Teilnehmer. Zertifizierungsstellen versehen digitale Zertifikate, die sie ausgeben, typischerweise mit einem Ablaufdatum und können außerdem ausgegebene Zertifikate ggf. widerrufen. Die Zugehörigkeit eines digitalen Zertifikats zu einer PKI wird mittels einer eigenen digitalen Signatur durch die Zertifizierungsstelle festgelegt.

Kryptografische Primitive und Protokolle Ein kryptografisches **Primitiv** ist eine grundlegende kryptografische Operation oder Funktion, die als Baustein für komplexere Systeme und Protokolle dient. Primitive führen einfache, genau definierte Aufgaben aus, beispielsweise Verschlüsselung (AES, RSA, Salsa20/ChaCha), kryptografisches Hashing (SHA-2, SHA-3, BLAKE) oder digitale Signaturen (RSA, ECDSA, EdDSA) und werden in verschiedenen Protokollen und Anwendungen eingesetzt.

Kryptografische **Protokolle** bezeichnen eine Abfolge von Regeln und Verfahren, die kryptografische Primitive nutzen, um bestimmte Sicherheitsaspekte wie Authentifizierung, Verschlüsselung oder Schlüsselaustausch umzusetzen. Diese Protokolle definieren, wie mehrere Parteien kommunizieren und kooperieren, um ihre Sicherheitsanforderungen zu erfüllen. Beispiele für kryptografische Protokolle sind TLS, das für verschlüsselte HTTPS-Verbindungen verwendet wird, oder das Authentifizierungsprotokoll Kerberos.

2.3 Datensparsamkeit

Datensparsamkeit in der Informatik bedeutet, dass nur die unbedingt notwendigen personenbezogenen oder -beziehbaren Daten erhoben, verarbeitet und gespeichert werden. Dieses Prinzip ist ein zentraler Bestandteil des Datenschutzes und der Privatsphäre. Die Registrierung eines Nutzers bei einem Online-Anbieter sollte beispielsweise nur grundlegenden Informationen wie einen Nutzernamen und, falls notwendig, ggf. eine E-Mail-Adresse zur Kontaktmöglichkeit verlangen, nicht jedoch zusätzliche Informationen wie Geburtsdatum, Telefonnummer oder Adressdaten, wenn diese nicht für die Nutzung der Dienste des Anbieters zwingend erforderlich sind. Entsprechend gespeicherte Daten dürfen nur für den festgelegten Zweck verwendet werden, für den sie ursprünglich erhoben wurden. Wenn Daten für einen neuen Zweck verwendet werden sollen, muss dies mit dem ursprünglichen Zweck vereinbar sein oder eine neue Einwilligung des betroffenen Nutzers eingeholt werden. Wo immer möglich, sollten personenbezogene Daten anonymisiert oder zumindest pseudonymisiert gespeichert werden, um eine Rückverfolgbarkeit von Aktivitäten des Nutzers einzuschränken und seine Identität zu schützen. Weiterhin sollten Daten von und über einen Nutzer nicht länger als notwendig gespeichert werden, d.h., sobald sie für ihren ursprünglichen Zweck nicht mehr benötigt werden, sollten sie sicher gelöscht werden. Nutzer sollten außerdem stets darüber informiert werden, welche Daten über sie erhoben werden und zu welchem Zweck. Eine ausdrückliche Einwilligung der Nutzer sollte eingeholt werden, bevor ihre Daten verarbeitet werden.

3 Konzept für eine datensparsame Altersverifikation

Das nachfolgend beschriebene Konzept für eine datensparsame Altersverifikation basiert auf einem Verfahren, das von den französischen Institutionen LINC[1], der École polytechnique und PEReN[2] entwickelt wurde [5].

Zunächst wird eine Übersicht über die Architektur mit den beteiligten Parteien gegeben, die für das Konzept notwendig sind. Anschließend wird der Prozess der datensparsamen Altersverifikation beschrieben und Schutzmechanismen erläutert, mit denen die zuvor definierten Schutzziele erreicht werden sollen. Danach werden die im Konzept verankerten Aspekte Datenschutz und Datensparsamkeit diskutiert und zuletzt mögliche Erweiterungen des Konzepts aufgeführt.

3.1 Architektur

Folgenden Parteien sind notwendig, um eine datensparsame Altersverifikation umzusetzen:

Nutzer Eine Person, die Dienste eines Anbieters im Internet nutzen möchte (beispielsweise durch den Besuch einer Webseite), die einen Altersnachweis erfordern. Der Nutzer möchte dazu gegenüber dem Anbieter nachweisen, dass er einer bestimmten Altersgruppe angehört (also beispielsweise volljährig ist oder jünger als 16 Jahre alt), dabei aber nur die dazu notwendigen Informationen über sich preisgeben. Der Nutzer muss mindestens einem Verifizierer bekannt sein und von diesem durch eine initiale einmalige Registrierung Zugangsdaten erhalten haben, um damit Altersnachweise anfordern zu können.

Anbieter Ein Anbieter von Diensten im Internet, die einen Altersnachweis erfordern. Der Anbieter möchte sicherstellen, dass er seine Dienste nur Nutzern zur Verfügung stellt, die nachweislich der für die jeweiligen Dienste erforderlichen Altersgruppe angehören. Dazu akzeptiert er Altersnachweise, die von Verifizierern zu diesem Zweck an Nutzer herausgegeben werden.

[1] Digital Innovation Lab der nationalen Datenschutzbehörde Frankreichs (CNIL)
[2] Kompetenzzentrum für digitale Regulierung

Verifizierer Eine Entität, etwa eine Behörde, eine Organisation oder ein Dienstleister, die das Alter von Nutzern verifizieren und Altersnachweise ausgeben kann. Ein Verifizierer möchte sicherstellen, dass ein Altersnachweis, den er für einen anfragenden Nutzer herausgibt, nur für diesen gültig ist, nicht unbemerkt verändert werden kann und außerdem von beliebigen Anbietern als gültig anerkannt wird. Damit der Verifizierer Altersnachweise für Nutzer herausgeben kann, müssen diese Nutzer ihm vorher bekannt sein und sich bei ihm für jede Altersanforderung authentifizieren[3]. Der Verifizierer muss innerhalb der für die Altersverifikation eingesetzten PKI von einer Zertifizierungsstelle die Berechtigung erhalten haben, als Verifizierer agieren zu dürfen.

Zertifizierungsstelle Eine Entität, beispielsweise eine Behörde, die kontrolliert, welche Entitäten als Verifizierer agieren dürfen, also gültige Altersnachweise ausstellen können. Die Zertifizierungsstelle kann die Berechtigung, als Verifizierer agieren zu dürfen, innerhalb einer **PKI**, die für die Altersverifikation eingesetzt wird, an neue Entitäten herausgeben und bestehende Berechtigungen zurückziehen, falls notwendig. Anbieter und Nutzer müssen der Zertifizierungsstelle vertrauen[4].

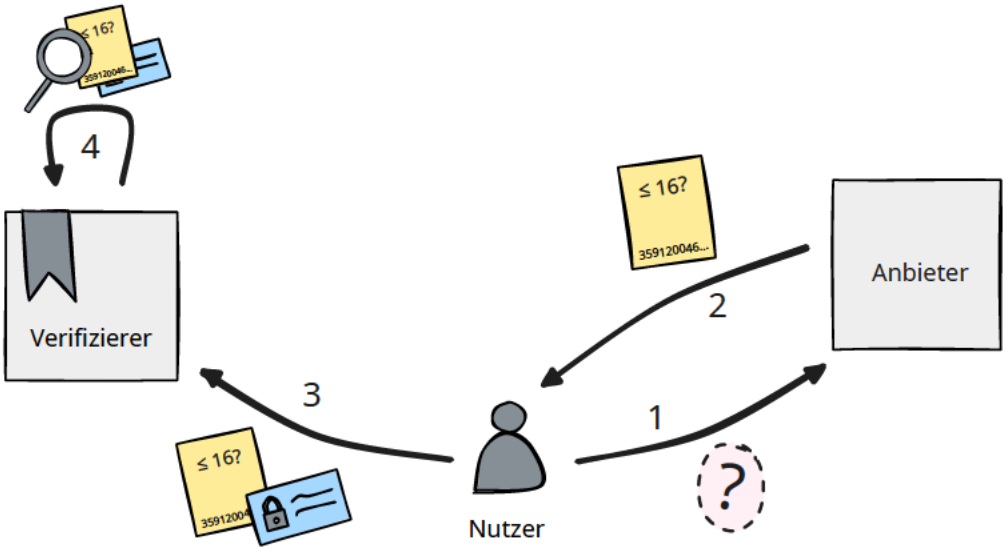
[3] Die Authentifizierung des Nutzers beim Verifizierer kann manuell über die Eingabe von Zugangsdaten oder automatisiert über Zugangstoken erfolgen, die beispielsweise nach einer einmaligen manuellen Authentifizierung an den Nutzer ausgegeben werden und für einen gewissen Zeitraum gültig sind.

[4] Vergleichbar mit Zertifizierungsstellen für gesicherte TLS-Verbindungen, die im Browser oder im Betriebssystem hinterlegt sind

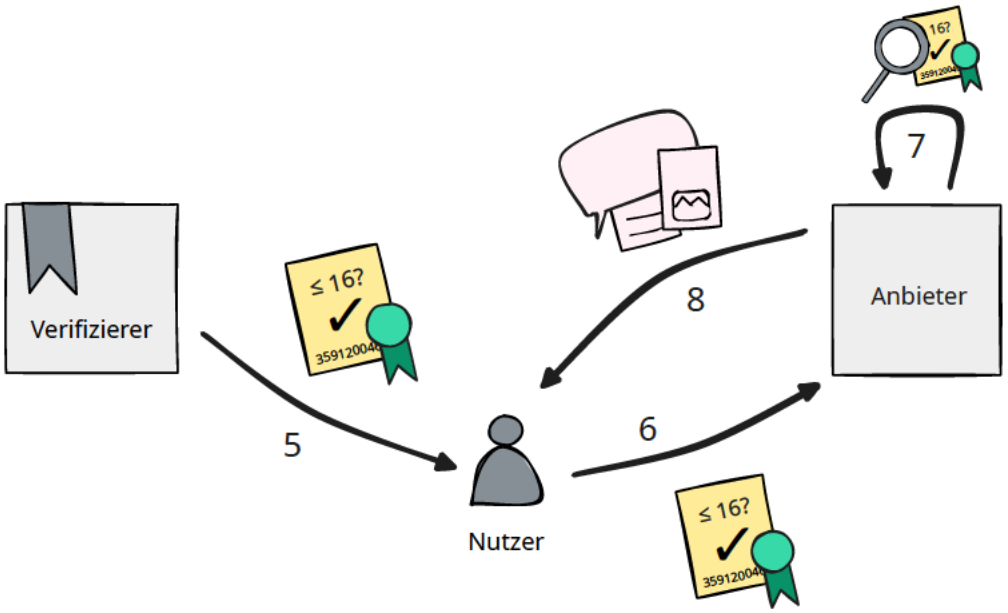
3.2 Verifikationsprozess

Nachfolgend werden die Prozessschritte zur datensparsamen Verifikation des Alters eines Nutzers, der auf altersbeschränkte Dienste eines Anbieters zugreifen möchte, beschrieben und in Abbildung 3.1 veranschaulicht:

1. Der Nutzer möchte Dienste eines Anbieters nutzen, die altersbeschränkt sind.
2. Der Anbieter fordert einen *Altersnachweis* an. Dazu schickt er an den Nutzer
   - die *Altersanforderung* zur Nutzung der gewünschten Dienste (z.B. »mindestens 18«, »höchstens 12«, »zwischen 16 und 18«) und
   - eine von ihm erstellte *Zufallszahl* in einem standardisierten Format mit einer zeitlich kurzen Gültigkeit (beispielsweise 60 Sekunden).
3. Der Nutzer authentifiziert sich gegenüber einem von ihm gewählten Verifizierer und schickt an diesen die Altersanforderung und die Zufallszahl, die er vom Anbieter erhalten hat. Anhand der Zufallszahl ist nicht erkennbar, von welchem Anbieter diese stammt.
4. Der Verifizierer prüft, ob der authentifizierte Nutzer die erhaltene Altersanforderung erfüllt.
5. Der Verifizierer signiert das Ergebnis der Prüfung sowie die Zufallszahl, die nun zusammen mit der gültigen digitalen Signatur den *Altersnachweis* bilden, und schickt diesen zurück an den Nutzer.
6. Der Nutzer leitet den Altersnachweis an den Anbieter weiter.
7. Der Anbieter kann anhand der Gültigkeit der digitalen Signatur des Verifizierers die Integrität und Authentizität des Altersnachweises und außerdem dessen Zugehörigkeit zum Nutzer feststellen, da die im Altersnachweis enthaltene, ebenfalls signierte Zufallszahl in diesem Zeitfenster ausschließlich diesem Nutzer übermittelt wurde. Die Gültigkeit der Signatur kann der Anbieter über die PKI prüfen.
8. Der Anbieter kann nun dem Nutzer Zugriff auf seine altersbeschränkten Dienste gewähren, falls der Altersnachweis belegt, dass die damit verbundene Altersanforderung erfüllt ist, der Nutzer also beispielsweise ein bestimmtes Mindestalter erreicht oder ein Maximalalter noch nicht erreicht hat. Der Anbieter benötigt keinerlei weitere Informationen vom Nutzer.



(a) Altersverifikationsprozess, Schritte 1–4



(b) Altersverifikationsprozess, Schritte 5–8

Abbildung 3.1:
Prozess für datensparsame Altersverifikation (Altersanforderung in Gelb, Altersnachweis in Gelb mit grünem Siegel, Zugangsdaten des Nutzers in Blau, Daten altersbeschränkter Dienste in Hellrot)

3.3 Schutzmechanismen

Für den zuvor beschriebenen Verifikationsprozess wird nachfolgend definiert, mit welchen konkreten Sicherheitsmaßnahmen die Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität erreicht werden können.

Vertraulichkeit Um sicherzustellen, dass kein unbefugter Zugriff durch Dritte auf die Kommunikation innerhalb des Verifikationsprozesses stattfinden kann, wird für jeglichen Datenaustausch zwischen den Kommunikationspartnern (also zwischen Nutzer und Anbieter und zwischen Nutzer und Verifizierer) Transportverschlüsselung mittels TLS eingesetzt, die nahezu flächendeckend im Internet mit dem HTTPS-Protokoll umgesetzt werden kann. Für den Einsatz von TLS ist keinerlei weitere Implementierung notwendig, bereits bestehende globale Infrastruktur kann direkt genutzt werden.

Für die Authentifizierung des Nutzers gegenüber dem Verifizierer ist ein sicheres Authentifizierungsverfahren notwendig, um zu verhindern, dass unbefugte Dritte sich als dieser Nutzer ausgeben, um an seiner statt Altersnachweise vom Verifizierer anzufordern und entgegenzunehmen. Hier wird vorgeschlagen, eine Authentifizierung mittels des OAuth-Protokolls einzusetzen. Dabei werden nach einer Authentifizierung des Nutzers beim Verifizierer zeitlich beschränkte Tokens ausgestellt, die dann innerhalb einer gewissen Zeitspanne für nachfolgende weitere Authentifizierungen bei der Anfrage von Altersnachweisen verwendet werden können. Die initiale Authentifizierung des Nutzers kann dabei über die Eingabe eines Benutzernamen und Passworts oder über ein passwortgeschütztes Client-Zertifikat erfolgen, wie es beispielsweise bei der Steuererklärung mit ELSTER bereits eingesetzt wird.

Um entsprechende Zugangsdaten (Benutzername und Passwort oder Client-Zertifikat) vom Verifizierer zu erhalten, muss sich der Nutzer dafür zuvor beim Verifizierer einmalig registrieren. In Abhängigkeit davon, ob bereits verifiziert korrekte Informationen über das Alters des Nutzers beim Verifizierer vorliegen oder nicht, kann dazu für den Nutzer ggf. notwendig sein, beispielsweise einmalig persönlich beim Verifizierer vorstellig zu werden und mit einem Ausweisdokument sein Alter zu belegen. Ebenso ist denkbar, das Alter mittels der Online-Ausweisfunktion des Personalausweises einmalig beim Verifizierer nachzuweisen. Allgemein sollen dabei bestehende Datensätze mit Altersinformationen verwendet werden, wie sie beispielsweise vom Bundeszentralamt für Steuern für jede Bürgerin und jeden Bürger erstellt werden, und somit keine neuen Datenbanken entstehen, in denen neue personenbeziehbare Datensätze gespeichert werden.

Integrität Die Integrität der Daten, die zwischen den Kommunikationspartnern ausgetauscht werden, wird mittels der eingesetzten Transportverschlüsselung über TLS gewährleistet. Die Integrität des Altersnachweises, den ein Veri-

fizierer ausstellt, kann sowohl vom Nutzer als auch von beliebigen Anbietern anhand der Gültigkeit der im Altersnachweis enthaltenen digitalen Signatur des Verifizierers überprüft werden.

Verfügbarkeit Die Verfügbarkeit einer datensparsamen Altersverifikation folgt unmittelbar aus der Verfügbarkeit des Verifizierers. Falls dieser in seiner Funktion nur eingeschränkt oder gar nicht erreichbar ist, kann durch ihn kein Altersnachweis ausgestellt werden und der Nutzer muss auf einen anderen Verifizierer ausweichen. Voraussetzung dafür ist, dass der Nutzer sich zuvor auch bei anderen Verifizieren registriert und dort entsprechende Zugangsdaten (Benutzername und Passwort oder Client-Zertifikat, siehe zuvor unter »Vertraulichkeit«) erhalten hat.

Um eine möglichst umfassende Verfügbarkeit zu gewährleisten, müssen Verifizierer für ihre Schnittstellen, die für die Kommunikation mit dem Nutzer vorgesehen sind, Vorkehrungen nach aktuellem Stand der Technik u.a. gegen unbefugten Zugriff und DDoS-Angriffe, für Load-Balancing, Redundanz und Failover sowie für geeignetes Backup, Alerting und Monitoring einsetzen.

Authentizität Die Authentizität der Kommunikationspartner muss bei der datensparsamen Altersverifikation an drei verschiedenen Stellen gewährleistet sein:

1. Bei jeder Datenübertragung
2. Bei der Anmeldung des Nutzers beim Verifizierer
3. Bei der Prüfung des Altersnachweises

Die Datenübertragung findet ausschließlich zwischen dem Nutzer auf der einen Seite und entweder dem Anbieter oder dem Verifizierer auf der anderen Seite statt. Hierbei muss für den Nutzer sicher nachvollziehbar sein, dass Anbieter bzw. Verifizierer authentisch sind und sich nicht beispielsweise um gefälschte Dienste handeln, die Altersnachweise des Nutzers ausspähen möchten, um diese anderweitig zu verwenden (Punkt 1). Die Authentizität kann hierbei durch die Nutzung von TLS zur Transportverschlüsselung erreicht werden, bei der eine Authentizitätsprüfung von Entitäten, die Dienste im Internet bereitstellen, teil des Protokolls ist. Jedoch wird auch ein gewisses Maß an Aufmerksamkeit vom Nutzer gefordert – so wie es bei quasi jeder Webseite im Internet der Fall ist, auf der Dienste genutzt oder Inhalte abgerufen werden können.

Weiterhin muss der Verifizierer sicherstellen können, dass der anfragende Nutzer, der einen Altersnachweis erhalten möchte, authentisch ist, also wirklich derjenige ist, für den der Verifizierer die Zugehörigkeit zu einer gewissen Alterskohorte nachweisen soll. Hierzu muss der Nutzer zwingend eine Authentifizierung mithilfe zuvor erhaltener Zugangsdaten durchführen (Punkt 2). Nach erfolgreicher Authentifizierung kann der Verifizierer davon ausgehen, dass die

Identität des anfragenden Nutzers mit derjenigen übereinstimmt, deren Daten ihm für einen Altersnachweis vorliegen.

Sowohl der Nutzer als auch der Anbieter müssen sicherstellen können, dass der Altersnachweis tatsächlich vom Verifizierer stammt und dieser berechtigt ist, entsprechende Altersnachweise auszustellen (Punkt 3). Dies kann durch die Nutzung der PKI zur Altersverifikation umgesetzt werden, bei der die Zertifizierungsstelle als zentrale Stelle definiert, welche Entitäten im Rahmen der PKI als Verifizierer agieren dürfen. Anhand einer gültigen digitalen Signatur kann somit belegt werden, dass der Verifizierer, der diese Signatur ausgestellt hat, sowohl authentisch als auch berechtigt ist.

3.4 Datenschutz und Datensparsamkeit

Der beschriebene Verifikationsprozess hat das Ziel, eine Altersverifikation zu ermöglichen, ohne dass der Verifizierer erfährt, für welchen Anbieter der Nutzer einen Altersnachweis benötigt. Der Verifizierer erfährt nur, für welchen Nutzer ein Altersnachweis erbracht werden soll sowie die zur Altersanforderung zugehörige kurzzeitig gültige Zufallszahl, die jedoch keine Rückschlüsse auf den Anbieter zulässt, der sie erzeugt hat. Diese Zufallszahl muss entsprechend in einem standardisierten Format vorliegen, also über alle Anbieter hinweg einheitlich aufgebaut sein. Abhängig von der konkreten Gültigkeitsdauer wäre beispielsweise eine Sequenz von 8 zufällig gewählten Bytes mit einer Gültigkeit von 60 Sekunden denkbar, sodass für Dritte das Erraten der korrekten Zufallszahl innerhalb ihres Gültigkeitszeitraums quasi auszuschließen ist.

Der Verifizierer muss gegenüber dem Anbieter als solche Entität bekannt sein, die berechtigt ist, das Alter von Personen zu verifizieren, also Altersnachweise auszugeben. Der Anbieter muss die digitale Signatur des Verifizierers und damit die Authentizität und Integrität ausgegebener Altersnachweise überprüfen können, was durch die eingesetzte PKI erreicht wird. Über die digitale Signatur wird somit für den Anbieter ersichtlich, welcher Verifizierer diese ausgestellt hat. Jede Entität, bei der der Nutzer und sein Alter bekannt sind und die eine digitale Signatur erzeugen kann, die innerhalb der PKI gültig ist und somit vom Anbieter akzeptiert wird, kann als Verifizierer agieren und vom Nutzer zur Altersverifikation angefragt werden. Der Nutzer kann hierzu auch beispielsweise verschiedene Verifizierer abwechselnd nutzen, bei denen er sich initial einmalig registriert hat.

Der Nutzer kann gegenüber dem Anbieter anonym bleiben, da er mittels der Altersverifikation nur nachweisen muss, dass er einer bestimmten Altersgruppe angehört. Er muss dazu kein Nutzerkonto erzeugen und auch keine weiteren Daten über sich preisgeben. Der Nutzer kann den Anbieter auch zusätzlich über das Tor-Netzwerk besuchen und somit seine IP-Adresse verschleiern, während er

aber trotzdem die beschriebene Altersverifikation durchführen kann. Seine Identität muss der Nutzer also nur gegenüber dem Verifizierer offenlegen, damit dieser sein Alter zur Erstellung von Altersnachweisen heranziehen kann.

Damit sich der Nutzer gegenüber dem Verifizierer authentifizieren kann, ist zwingend notwendig, dass er eine initiale einmalige Registrierung beim Verifizierer vornimmt. Hierzu muss der Nutzer gegenüber dem Verifizierer seine Identität offenbaren und beispielsweise mittels eines Ausweisdokuments sein Alter zweifelsfrei nachweisen. Dies kann durch eine persönliche Vorstellung beim Verifizierer durchgeführt werden. Zentraler Aspekt bei der Registrierung bei einem Verifizierer ist, dass dort keine neuen personenbeziebaren Datenbestände über den Nutzer angelegt werden sollen, sondern auf Bestandsdaten zurückgegriffen werden soll, die dem Verifizierer bereits vorliegen – beispielsweise bei einen (als Verifizierer agierenden) Einwohnermeldeamt, bei dem der Nutzer samt seines Alters bereits durch seine Anmeldung bekannt ist. Der Nutzer kann dann vom Verifizierer seine persönlichen Zugangsdaten erhalten, über die er Altersnachweise anfragen kann.

3.5 Benutzbarkeit

Für den Nutzer einer datensparsamen Altersverifikation existieren mehrere Möglichkeiten, um in seiner Rolle als notwendiger Kommunikationsteilnehmer mit Anbieter und Verifizierer die beschriebenen Schritte durchzuführen. Hierbei ist eine Software-Lösung sinnvoll, die den Nutzer beim Datenaustausch unterstützen und ein komfortables Nutzererlebnis bieten soll. Zur Demonstration des beschriebenen Konzepts wird eine Browser-Extension implementiert, die für Nutzer einfach zu installieren und zu verwenden sein soll. Ebenso können auch andere Software-Lösungen implementiert werden, beispielsweise eine App für Smartphones.

Als erster Schritt ist für den Nutzer notwendig, die Browser-Extension aus einer vertrauenswürdigen Quelle zu installieren, beispielsweise aus dem Browserzugehörigen Repository für Extensions wie Mozilla Addons oder dem Chrome Web Store. Nach der Installation wird der Nutzer aufgefordert, aus einer Liste der verfügbaren Verifizierer diejenigen auszuwählen, für die er durch eine vorangegangene Registrierung Zugangsdaten besitzt, also beispielsweise ein Client-Zertifikat oder Benutzernamen und Passwort. Weiterhin bekommt der Nutzer die Möglichkeit, sich über die Browser-Extension benachrichtigen zu lassen, wenn eine Altersanforderung an ihn gestellt wird oder diese Benachrichtigungen für eine gewisse Zeit zu unterdrücken.

Sobald der Nutzer nun bei einem Anbieter nach altersbeschränkten Diensten fragt, bekommt er über die Browser-Extension eine Meldung, dass eine Altersanforderung an ihn gestellt wurde, die ihm entsprechend angezeigt wird. Er bekommt dann die Möglichkeit, diese Altersanforderung zu blockieren oder an einen der von ihm zuvor konfigurierten Verifizierer weiterzuleiten. Entscheidet

sich der Nutzer für das Blockieren der Altersanforderung, kann er die altersbeschränkten Dienste nicht nutzen. Leitet er die Anforderung weiter, wird er zur Eingabe seiner Zugangsdaten beim Verifizierer aufgefordert (beispielsweise einmal pro Tag) und kann dann entscheiden, ob er weitere Altersanforderungen transparent an seinen Verifizierer weiterleiten möchte, ohne diese jeweils bestätigen zu müssen oder ob er weiteren Altersanforderungen einzeln zustimmen möchte. Für bestimmte Altersanforderungen kann auch zwingend eine Zustimmung des Nutzers eingeholt werden – etwa, wenn sich seine Zugehörigkeit zu einer Alterskohorte gegenüber einem längerfristig genutzten Anbieter ändert, sodass dieser durch eine erneute Altersanforderung und dem damit verbundenen, nun geänderten Altersnachweis potenziell das Geburtsjahr des Nutzers ermitteln könnte (siehe dazu auch Abschnitt 3.6).

Nach erfolgreicher erster Anmeldung beim Verifizierer wird in der Browser-Extension ein zeitlich begrenzter Zugangstoken hinterlegt, der über einen gewissen Zeitraum hinweg erlaubt, sich für Altersanforderungen beim Verifizierer zu authentifizieren, ohne sich erneut mit Zugangsdaten anmelden zu müssen. Nach Ablauf des Zugangstokens (beispielsweise nach Ablauf von 24 Stunden) muss dieser durch den Nutzer dann unter Eingabe seiner Zugangsdaten wieder erneuert werden.

Anbieter können nun weiter Altersanforderungen an den Nutzer in regelmäßigen Abständen schicken (beispielsweise alle 15 Minuten), die der Nutzer dann entweder manuell begutachten und anschließend entweder weiterleiten oder blockieren kann oder die vollständig transparent für den Nutzer automatisch an den Verifizierer weitergeleitet werden. Dabei bleibt der Nutzer stets über ggf. automatisch weitergeleitete Altersanforderungen informiert und kann anhand eines Protokolls innerhalb der Browser-Extension einsehen, wann, wie oft und von wem die Altersanforderungen eingingen und welche Altersnachweise er vom Verifizierer entgegennehmen konnte.

Der Nutzer hat auch die Möglichkeit, sich auf eigenen Wunsch bereits vor dem zeitlichem Ablauf des in der Browser-Extension temporär gespeicherten Zugangstokens vom Verifizierer abzumelden, sodass er sich in jedem Fall bei der nächsten Altersanforderung erneut beim Verifizierer unter Eingabe seiner Zugangsdaten authentifizieren muss.

3.6 Mögliche Erweiterungen

Zur Erweiterung des Konzepts sind verschiedene zusätzliche Aspekte denkbar, deren Umsetzung nachfolgend diskutiert wird:

Anonymität von Verifizierern Im beschriebenen Konzept ist der Verifizierer, der einen Altersnachweis ausstellt, für den Anbieter, der diesen vom Nutzer erhält, ersichtlich. Aus diesem Umstand lässt sich für den Anbieter ggf. eine örtliche Nähe des Nutzers zum Verifizierer ableiten, also beispielsweise, aus welchem Land der (ansonsten für ihn anonyme) Nutzer stammen könnte. Diese Information ist zwar für den Anbieter auch typischerweise anhand der IP-Adresse des Nutzers ersichtlich, hier kann der Nutzer aber zusätzliche Maßnahmen ergreifen, um diese zu verschleiern. Diese Möglichkeit ist ihm bei Altersnachweisen und den digitalen Signaturen darauf nicht gegeben.

Um zu erreichen, dass der Verifizierer gegenüber dem Anbieter anonym bleibt, schlagen die französischen Autoren des Verfahrens, auf dem das vorgestellte Konzept basiert, vor, *Group Signatures* für Altersnachweise einzusetzen. Hierbei bilden Verifizierer eine Gruppe, in der jedes Mitglied digitale Signaturen für Altersnachweise ausstellen kann. Den Signaturen ist dabei jedoch nicht anzusehen, welches Mitglied (Verifizierer) innerhalb der Gruppe signiert hat, sodass der Anteil an Informationen, der den Anbieter mit dem Altersnachweis erreicht, reduziert wird: Dieser sieht lediglich, dass aus einer Gruppe von Verifizierern einer einen Altersnachweis ausgestellt hat.

Group Signatures erfordern einen *Group Manager*, der zum einen für das Hinzufügen und Entfernen von Mitgliedern (Verifizierern) einer Gruppe zuständig ist und zum anderen als einzige Partei die Möglichkeit besitzt, die Identität eines Verifizierers, der eine digitale Signatur erstellt hat, innerhalb einer Gruppe aufzudecken. Diese Möglichkeit zur Aufdeckung ist auch für die datensparsame Altersverifikation notwendig, um ggf. Verifizierer zu sperren, die fehlerhafte Altersnachweise ausstellen und beispielsweise jede Altersanforderung positiv bestätigen.

Nachteil von Group Signatures innerhalb der Altersverifikation ist eine deutliche Erhöhung die Komplexität der eingesetzten Signaturverfahren und der Organisation von Verifizierern innerhalb der PKI (Gruppenbildung, Gruppen-Management, Revocation-Prozess). Im Gegenzug dazu tragen Group Signatures signifikant zur Datensparsamkeit bei.

Skalierbare Zuverlässigkeit der Altersprüfung Als Erweiterung ist bei der datensparsamen Altersverifikation auch die Umsetzung einer skalierbaren Zuverlässigkeit dahingehend denkbar, wie genau das Alter des Nutzers initial vom Verifizierer überprüft wird [9]: Wenn ein Anbieter Dienste zur Verfügung stellen möchte, die einen besonders sorgfältig geprüften Altersnachweis erfordern, könnte er beispielsweise nur Altersnachweise von Verifizierern akzeptieren, für

die der Nutzer bei der initialen einmaligen Registrierung zum Identitätsnachweis persönlich vorstellig werden und ein Ausweisdokument mit Altersangabe vorlegen musste. Entsprechend »schwächere« Altersnachweise, bei denen der Identitätsnachweis des Nutzers beim Verifizierer beispielsweise zeitlich länger zurückliegt oder nicht unmittelbar durch Vorlage eines Ausweisdokuments durchgeführt wurde, könnten dann ggf. von Banken, Krankenkassen oder durch den Arbeitgeber erbracht werden. Entsprechend wären hier verschiedene Zertifizierungsstufen für Verifizierer denkbar.

Verschleierung von Altersanforderungen Altersanforderungen, die von einem Nutzer an einen Verifizierer geschickt werden, können potenziell Hinweise darauf geben, auf welche Art von Diensten der Nutzer zugreifen möchte. Schickt beispielsweise ein minderjähriger Nutzer in kurzen Zeitabständen regelmäßig Altersanforderungen wie »Volljährigkeit erreicht« an den Verifizierer, so könnte dieser daraus schließen, dass und auch wann genau der Nutzer Zugang zu für ihn noch nicht geeignete Dienste erhalten möchte.

Um die angefragte Alterskohorte, deren Zugehörigkeit im Rahmen einer Altersanforderung geprüft werden soll, vor dem Verifizierer zu verschleiern, ist folgende Erweiterung denkbar:

1. Der Nutzer nimmt (automatisch mittels Browser-Erweiterung, Mobile App, etc.) die Altersanforderung des Anbieters entgegen (Schritt 2 im Altersverifikationsprozess).
2. Der Nutzer generiert (ebenfalls automatisch) zusätzliche Altersanforderungen zu weiteren unterschiedlichen Alterskohorten und mit neuen Zufallszahlen. Beispielsweise erzeugt der Nutzer zur Altersanforderung »maximal 16 Jahre alt«, die er vom Anbieter erhalten hat, weitere Altersanforderungen wie »mindestens 16 Jahre alt«, »Volljährigkeit erreicht«, »zwischen 12 und 15 Jahre alt« usw.
3. Der Nutzer schickt diese Sammlung an Altersanforderungen an den Verifizierer (Schritt 3 im Altersverifikationsprozess), der somit nicht mehr erkennen kann, welche Altersanforderung eigentlich diejenige ist, die für den Nutzer relevant ist und vom Anbieter übermittelt wurde.
4. Der Verifizierer prüft alle Altersanforderungen und beantwortet und signiert diese entsprechend (Schritt 4 im Altersverifikationsprozess).
5. Der Nutzer nimmt die somit erbrachten Altersnachweise entgegen (Schritt 5 im Altersverifikationsprozess) und verwirft diejenigen Altersnachweise, die er nicht benötigt.
6. Der Nutzer schickt nur den Altersnachweis an den Anbieter (Schritt 6 im Altersverifikationsprozess), zu dem er ursprünglich die Altersanforderung erhalten hat (hier: »Maximal 16 Jahre alt«).

Nachteil dieser Erweiterung ist, dass der Aufwand zur Erstellung von Altersnachweisen für den Verifizierer signifikant steigt, da er pro Altersanforderung immer mehrere Prüfungen durchführen und Signaturen erstellen muss.

Verschleierung des Geburtsdatums in Grenzfällen Für den Nutzer ergeben sich im Rahmen einer datensparsamen Altersverifikation Grenzfälle, anhand derer Anbieter potenziell das exakte Geburtsdatum in Erfahrung bringen können: Fragt beispielsweise ein Nutzer kurz vor seinem Geburtstag, an dem sich seine Zugehörigkeit zu einer Alterskohorte ändert (beispielsweise 18. Geburtstag), bei einem Anbieter nach Diensten, für die er volljährig sein muss, und wiederholt eine solche Anfrage direkt an seinem Geburtstag erneut, so kann der Anbieter sein Geburtsdatum anhand entsprechend erbrachter Altersnachweise ableiten. Voraussetzung hierfür ist, dass der Anbieter den Nutzer über mehrere Tage hinweg beispielsweise über Cookies o.ä. trackt, ihn also als denselben Nutzer identifizieren kann, der zuvor noch nicht 18 Jahre alt war, als er erstmalig nach Zugang zu den Diensten gefragt hatte.

Um dem entgegenzuwirken, kann zum einen der Nutzer Möglichkeiten nutzen, die ein Tracking durch den Anbieter erschweren oder unmöglich machen (privater Browser-Tab, Änderungen seiner IP-Adresse, Nutzung des Tor-Browsers), sodass der Anbieter keine Möglichkeit hat, bei Altersnachweisen, die er über mehrere Tage erhält, zu erkennen, dass diese vom selben Nutzer geschickt werden. Somit wäre dann auch eine Änderung der Zugehörigkeit zu einer Alterskohorte (wenn der Nutzer beispielsweise 18 Jahre alt geworden ist) durch den Anbieter als solche nicht zu erkennen.

Zum anderen kann bei der datensparsamen Altersverifikation auf Seite des Verifizierers der Prozess zur Ausstellung des Altersnachweises abgeändert werden, sodass für den Anbieter zumindest eine entsprechende Ableitung des genauen Geburtsdatums des Nutzers eingeschränkt wird: Der Verifizierer könnte für Altersanforderungen, die er vom Nutzer erhält, grundsätzlich nicht tagesgenaue, sondern restriktivere, »unscharfe« Altersnachweise erzeugen. Beispielsweise könnte der Verifizierer in einem zufälligen Zeitraum (z.B. einige Monate) *vor* dem 16. Geburtstag des Nutzers (also dem Beginn des 17. Lebensjahrs) eine Altersanforderung »Maximal 16 Jahre alt« bereits mit »Nein« beantworten und digital signieren. Ebenso könnte der Verifizierer die Altersanforderung »Volljährigkeit erreicht« erst in einem zufälligen Zeitraum *nach* dem 18. Geburtstag des Nutzers mit »Ja« beantworten und digital signieren. Somit wäre für den Anbieter das exakte Geburtsdatum nicht mehr ableitbar, bliebe aber auf einen bestimmten Zeitraum und ggf. das entsprechende Jahr eingrenzbar. Zusätzlich müsste der Nutzer die damit verbundenen Restriktionen hinnehmen, dass er bestimmte altersbeschränkte Dienste schon früher nicht mehr bzw. erst mit Verspätung nutzen kann.

4 Umsetzungsmöglichkeiten

4.1 Umsetzung als Browser-Extension

Zu dem vorliegenden Konzept wird eine Browser-Extension entwickelt, die die technische Umsetzung des Konzepts demonstrieren soll. Die Browser-Extension wird für einen gängigen Webbrowser (Mozilla Firefox oder Google Chrome) implementiert und übernimmt dabei wesentliche Funktionen beim Datenaustausch zwischen Nutzer und Anbieter sowie zwischen Nutzer und Verifizierer. Mithilfe der Browser-Extension kann der Nutzer Verifizierer auswählen, zu denen er Zugangsdaten besitzt, die er bei einer initialen einmaligen Registrierung von diesen erhalten hat. Der Nutzer kann sich dann bei einer Altersanforderung, die er zugeschickt bekommt, beim Verifizierer mit seinen Zugangsdaten authentifizieren, wodurch dann nach erfolgreicher Authentifizierung in der Browser-Extension ein zeitlich begrenzter Zugangstoken hinterlegt wird. Somit muss der Nutzer innerhalb des Gültigkeitszeitraums des Tokens nicht für jede weitere Altersanforderung erneut eine manuelle Authentifizierung beim Verifizierer durchführen. Altersanforderungen werden in der Browser-Extension protokolliert und können jederzeit vom Nutzer eingesehen werden. Zu keinem Zeitpunkt werden in der Browser-Extension Informationen über das Alter des Nutzers gespeichert. Altersnachweise werden bei der datensparsamen Altersverifikation ausschließlich von Verifizierern ausgestellt und nur dort liegen Informationen über das Alter des Nutzers vor.

4.2 Umsetzung als Mobile App

Analog zur Umsetzung als Browser-Extension ist die Entwicklung einer App für Smartphones möglich, die die gleiche Funktionalität übernimmt: Sobald der Nutzer von einem Anbieter, dessen Dienste er mit dem Smartphone nutzen möchte, eine Altersanforderung erhält, kann er eine entsprechende App für die datensparsame Altersverifikation nutzen, um sich bei einem Verifizierer seiner Wahl (von dem er zuvor Zugangsdaten erhalten hat) zu authentifizieren und einen Altersnachweis zu erhalten, der dann über die App wieder zurück an den Anbieter geschickt wird. Auch hier werden zu keinem Zeitpunkt Informationen über das Alter des Nutzers in der App gespeichert.

4.3 Weitere Umsetzungsmöglichkeiten

Das Konzept lässt sich bei Bedarf von den vorgeschlagenen Kommunikationswegen loslösen und auch anderweitig implementieren. So wäre es auch möglich, beispielsweise vollständig manuell eine datensparsame Altersverifikation durchzuführen, ohne eine App oder eine Browser-Extension einzusetzen: Hierbei könnte der Anbieter dem Nutzer eine Altersanfrage als »Rohdaten« anzeigen (beispielsweise als Zeichenkette oder kodiert als QR- oder JAB Code[1]), der Nutzer könnte die Altersanforderung dann im Browser kopieren (oder den entsprechenden Code einscannen und die Daten auslesen) und an einen Verifizierer seiner Wahl weiterleiten. Der Verifizierer könnte dann nach Prüfung und Ausstellung des Altersnachweises diese Daten erneut dem Nutzer als Rohdaten anzeigen, die dieser dann wiederum kopiert und an den Anbieter weiterleitet.

Ein so umgesetzter Prozess zur Altersverifikation wäre natürlich nicht sehr nutzerfreundlich, würde ein geringeres Sicherheitsniveau liefern (siehe dazu Kapitel 5) und wäre gerade für regelmäßig wiederkehrende Altersanforderungen dem Nutzer nicht zumutbar, soll hier aber lediglich demonstrieren, dass das Konzept selbst flexibel an verschiedene Einsatzumgebungen angepasst werden kann, die durchaus stark voneinander abweichen können.

[1] JAB Code – »Just Another Bar Code«: https://jabcode.org/

5 Herausforderungen

5.1 Festlegung einer zentralen Zertifizierungsstelle

Für die datensparsame Altersverifikation ist die Implementierung einer PKI mit einer zentralen, staatliche beauftragten, unabhängigen Zertifizierungsstelle notwendig, die keinerlei kommerzielle Interessen verfolgt und Verifizierer neutral und fachkundig prüfen kann. Eine länderübergreifende Nutzung der datensparsamen Altersverifikation wird nicht mit einer einzigen Zertifizierungsstelle möglich sein und wäre sicherheitstechnisch nicht zu empfehlen (»Single Point of Failure«). Vielmehr ist naheliegend, länderspezifische Zertifizierungsstellen zu etablieren, die für die Prüfung und Zertifizierung nationaler Verifizierer zuständig sind. Hierzu wäre einmalig die Festlegung eines länderübergreifend gültigen Verzeichnisses notwendig, in dem alle länderspezifischen Zertifizierungsstellen erfasst sind. Auf nationaler Ebene könnten dann die jeweiligen Zertifizierungsstellen ihre Aufgaben bzgl. Erteilung und Widerruf von Berechtigungen für Verifizierer wahrnehmen. Nutzer der datensparsamen Altersverifikation wären weiterhin ungebunden an bestimmte Länder und könnten sich potenziell beliebige Verifizierer aussuchen, um sich dort zu registrieren (maßgeblich abhängig davon, wie der konkrete Registrierungsprozess gestaltet ist). Wesentliche Herausforderung für eine zentrale Zertifizierungsstelle (mindestens pro Land) ist die Festlegung der dafür infrage kommenden Institution und die Integration in bereits bestehende organisatorische und technische Strukturen.

5.2 Ausspähung von Zugangsdaten

Wie bei allen Prozessen, bei denen eine Authentifizierung über das Internet durchgeführt wird, besteht auch im Rahmen des datensparsamen Altersverifikationsprozesses die Gefahr, dass sich unbefugte Dritte Zugriff auf die Zugangsdaten eines Nutzers verschaffen, die dieser verwendet, um sich bei einem Verifizierer zu authentifizieren und dort Altersnachweise zu erhalten. Besonders in einem Umfeld, in dem unbefugte Dritte beispielsweise durch räumliche Nähe und / oder durch existierende Abhängigkeitsverhältnisse Kontrolle über Teile des Altersverifikationsprozesses oder über die dazu eingesetzten Geräte des Nutzers erlangen können, ist technisch nahezu unmöglich, die Ausspähung von Zugangsdaten zu verhindern. Dennoch können zur Vorbeugung Sicherheitsvorkehrungen getroffen werden:

Durchgängige Transportverschlüsselung Die Übertragung jeglicher Kommunikationsdaten im Altersverifikationsprozess erfolgt durchgängig verschlüsselt. Authentische Verifizierer können im Rahmen der PKI automatisch vom Nutzer als solche erkannt werden.

Mehrstufige Authentifizierung Die Verwendung einer mehrstufigen Authentifizierung bei Verifizierern ist zu empfehlen, etwa eine Kombination aus Zugangsdaten und einem *Time-based One-Time Password (TOTP)* als weiteren Faktor, der mit dem Smartphone erzeugt werden kann.

Protokollierung beim Verifizierer Eine Protokollierung der Altersanforderungen sowie aller Geräte, die beim Verifizierer für den datensparsamen Altersverifikationsprozess freigeschaltet sind, ist auf der Seite des Verifizierers zu empfehlen. Somit kann der Nutzer stets die Übersicht behalten, zu welchen Zeitpunkten in seinem Namen Altersanforderungen an den Verifizierer geschickt werden und welche Geräte dabei involviert sind. Im Falle unberechtigter Zugriffe kann der Nutzer dann (ggf. in Zusammenarbeit mit dem Verifizierer) reagieren.

Aufklärung über Sensibilität von Zugangsdaten Nutzer müssen bezüglich der Zugangsdaten, die sie von Verifizierern erhalten, umfassend aufgeklärt und dahingehend sensibilisiert werden, diese mit keiner weiteren Person – auch nicht mit Vertrauenspersonen – zu teilen (vergleichbar mit der PIN für die Bankkarte oder mit dem Passwort für das ELSTER-Zertifikat zur Steuererklärung). Entsprechend ist auch notwendig, geeignete Prozesse zu etablieren, die es insbesondere minderjährigen Nutzern ermöglichen, Zugangsdaten persönlich von Verifizierern zu erhalten und ausschließlich für sich zu nutzen.

5.3 Weitergabe von Zugangsdaten

Wie bereits im vorigen Abschnitt beschrieben, ist technisch nicht vollständig zu verhindern, dass Zugangsdaten zu einem Verifizierer durch Dritte ausgespäht werden können. Insbesondere kann eine freiwillige Weitergabe der eigenen bzw. die Verwendung anderer Zugangsdaten nicht verhindert werden, wie folgendes Beispiel demonstriert:

1. Nutzer A möchte bei einem Anbieter auf Dienste zugreifen, für die er keinen Altersnachweis erhalten würde, da er sich nicht in der dafür notwendigen Alterskohorte befindet.
2. Nutzer A nimmt die vom Anbieter erhaltene Altersanforderung entgegen und leitet diese an einen ihm bekannten Nutzer B weiter, der das passende Alter hat.

3. Nutzer B nutzt diese weitergeleitete Altersanforderung, um sich mittels eines Verifizierers einen eigenen Altersnachweis ausstellen zu lassen.
4. Nutzer B schickt den erhaltenen Altersnachweis an Nutzer A.
5. Nutzer A schickt den Altersnachweis, der eigentlich Nutzer B zugeordnet ist, an den Anbieter, der ihm daraufhin (unberechtigterweise) Zugriff auf die altersbeschränkten Dienste gewährt.

Dieses Angriffsszenario lässt sich schwer verhindern, wenn die Anonymität des Nutzers bestehen bleiben soll, wie sie in der datensparsamen Altersverifikation vorgesehen ist. Aufgrund der Tatsache, dass keine weiteren personenbeziehbaren Daten über den Nutzer vom Verifizierer zum Anbieter gelangen sollen, ist für den Anbieter nicht möglich, zweifelsfrei festzustellen, wer genau den Altersnachweis erbracht hat, sobald der Nutzer die Altersanforderung samt Zufallszahl Dritten mitgeteilt hat. Zusätzliche Informationen über den Nutzer, die der Anbieter bzw. der Verifizierer in die Altersanforderung bzw. den Altersnachweis integrieren könnten, um eine stärkere Verknüpfung mit dem beim Anbieter anfragenden Nutzer zu schaffen, lassen sich ebenfalls weitergeben oder übernehmen und schaffen kein höheres Maß an Sicherheit. Es wäre technisch sogar möglich, einen Proxy-Dienst zu entwickeln, der im Auftrag für beliebige Nutzer Altersanforderungen von Anbietern entgegennimmt, sich entsprechende Altersnachweise erstellen lässt und somit den Nutzern Zugriff auf Dienste bietet, der ihnen ansonsten nicht gestattet wäre.

Um eine Weitergabe von Zugangsdaten zumindest einzuschränken, kann zum einen der Zugriff auf die konkrete Altersanforderung samt Zufallszahl bzw. auf einen erhaltenen Altersnachweis durch diejenige Komponente, die der Nutzer dafür einsetzt (beispielsweise eine Browser-Extension oder eine Mobile App), insofern erschwert werden, dass diese nicht ohne größeren Aufwand aus der Komponente extrahiert und weitergegeben werden können. Zum anderen kann die Dauer, die die in der Altersanforderung enthaltene Zufallszahl gültig ist, möglichst gering gehalten werden (beispielsweise einige wenige Sekunden), sodass eine zusätzliche Weitergabe und Erstellung eines Altersnachweises durch Dritte jedenfalls eine zeitliche Herausforderung darstellen würde.

5.4 Länderspezifische Rechtslagen

Die gesetzlichen Vorgaben und Altersgrenzen für die Nutzung von Diensten im Internet sind je nach Land ggf. unterschiedlich. Obwohl eine länderübergreifende Harmonisierung und Kooperation wünschenswert wäre, ist die Entwicklung eines datensparsamen Altersverifikationsprozesses, der global allen rechtlichen und digitalen Anforderungen gerecht wird, eine sehr große Herausforderung. Die gegenwärtige Situation ist dadurch geprägt, dass es in einzelnen Ländern unterschiedliche Regulierungen gibt, wodurch sich Schlupflöcher ergeben. Insbesondere lassen sich folgende Problemstellungen formulieren:

International agierende Anbieter Bei großen Anbietern, die international ihre Plattformen betreiben und Nutzern aus vielen verschiedenen Ländern Dienste zur Verfügung stellen, ist eine homogene Altersverifikation nur begrenzt durchführbar. Dies würde entweder die Anwendung der strengsten rechtlichen Vorgaben für alle Nutzer oder aber länderspezifische Lösungen und damit wiederum eine robuste Erkennung der Herkunft von Nutzern erfordern, die auf die Dienste des Anbieters zugreifen möchten. Dabei ist absehbar, dass Anbieter wahrscheinlich kein starkes Eigeninteresse entwickeln werden, ohne rechtliche Verpflichtungen entsprechende Lösungen auf ihrer Seite zu implementieren.

Umgehung durch VPN- oder Proxy-Dienstleister In Ländern, in denen hohe Anforderungen an eine Altersverifikation für den Kinder- und Jugendschutz gestellt werden, kann der Zugriff auf altersbeschränkte Dienste effektiv umgesetzt werden. Allerdings besteht technisch die Möglichkeit, entsprechende Altersverifikationen zu umgehen, indem VPN- oder Proxy-Dienstleister aus Ländern mit weniger hohen Anforderungen für den Zugriff auf altersbeschränkte Dienste genutzt werden. Dies lässt sich im Rahmen der datensparsamen Altersverifikation nicht verhindern. Denkbar ist hier, Anbieter von Diensten in die Pflicht zu nehmen, eine robuste Erkennung von Nutzern entsprechender VPN- und Proxy-Dienstleister zu implementieren, um dann an diese striktere Altersanforderungen zu stellen, die sich an rechtlichen Altersbeschränkungen orientieren, wie sie beispielsweise in der EU gültig sind.

Literatur

[1] Wolfgang Böse u. a. »Internet-Versandhandel mit Alkohol: wird im Jugendschutz mit zweierlei Maß gemessen?« In: *Sucht* 56 (2010), S. 397–398.

[2] Andreas Büsch und Benedikt Geyer. »Zwischen Jugendmedienschutz und ›Porno-Kompetenz‹, Herausforderungen der Pornografisierung«. In: *Communicatio Socialis* 49.3 (2016), S. 269–282.

[3] Deutsche Post. *Postident für Privatkunden: FAQ*. https://www.deutschepost.de/de/p/postident/privatkunden/faq.html. Letzter Zugriff: 07.06.2024.

[4] Kathleen L Egan, Sophia Villani und Eric K Soule. »Absence of age verification for online purchases of cannabidiol and delta-8: implications for youth access«. In: *Journal of Adolescent Health* 73.1 (2023), S. 195–197.

[5] Jérôme Gorin, Martin Biéri und Côme Brocas. *Demonstration of a privacy-preserving age verification process*. https://linc.cnil.fr/demonstration-privacy-preserving-age-verification-process. Letzter Zugriff: 11.07.2024. 2022.

[6] Joachim von Gottberg. »Eine unendliche Geschichte. Porno-Portale aus Zypern weiterhin frei zugänglich«. In: *JMS Jugend Medien Schutz-Report* 45.4 (2022), S. 7–10.

[7] Herfurtner Rechtsanwaltsgesellschaft mbH. *Einwohnermeldeamt: Rechtliche Aufgaben und Zuständigkeiten*. https://kanzlei-herfurtner.de/einwohnermeldeamt/. Letzter Zugriff: 07.06.2024.

[8] Angelika Heyen und Carole Possing. »Aktuelle Problemfelder und Herausforderungen im Jugendmedienschutz«. In: *AfP* 54.1 (2023), S. 12–18.

[9] Chelsea Jarvie und Karen Renaud. »Are you over 18? A snapshot of current age verification mechanisms«. In: *2021 Dewald Roode Workshop*. 2021.

[10] Richard Joos. »Wie funktioniert der Pornografiemarkt im Internet?« In: *Zeitschrift für Sexualforschung* 30.01 (2017), S. 58–73.

[11] Tobias Keber. »Datenschutz und Mediensystem–Altersverifikation und Uploadfilter aus intradisziplinärer Perspektive«. In: *Abschlussmagazin des DFG-Graduiertenkollegs 1681/2» Privatheit & Digitalisierung*« (2021), S. 56–61.

[12] Mark Kesselmann. *Video Ident Verfahren: Digitaler Schlüssel für sichere E-Signaturen*. https://www.d-velop.de/blog/prozesse-gestalten/video-ident-verfahren/. Letzter Zugriff: 07.06.2024.

[13] Andreas van Loock. *Altersprüfung & IdentitätsCheck als Rund-um-sorglos-Paket*. https://www.fraspy.com/alterspruefung-identitaetscheck-als-rund-um-sorglos-paket/. Letzter Zugriff: 07.06.2024.

[14] Marian Margraf. *Der elektronische Identitätsnachweis: Einsatzmöglichkeiten des neuen Personalausweises im privat-wirtschaftlichen Umfeld*. Technische Hochschule Wildau, 2014.

[15] Cornelia Möhring. *Das Video-Ident-Verfahren: Was ist das und wie benutze ich es?* https://www.heise.de/tipps-tricks/Das-Video-Ident-Verfahren-Was-ist-das-und-wie-benutze-ich-es-4036733.html. Letzter Zugriff: 07.06.2024.

[16] Victoria Nash u. a. »Effective age verification techniques: Lessons to be learnt from the online gambling industry«. In: *Available at SSRN 2658038* (2012).

[17] Jan Pfeiffer. »OVG NRW: Untersagung pornografischer Internetangebote aus Zypern«. In: *Computer und Recht* 38.10 (2022), r117–r118.

[18] Ingrid Stapf und Jessica Heesen. »Kinder-und Jugendmedienschutz im Lichte der Kinderrechte: ethische Überlegungen zur Online-Sicherheit von Kindern und Jugendli-chen«. In: *BPJMAKTUELL* 2.2022 (2022), S. 14–22.

[19] Christine W Trültzsch-Wijnen. »UN-Kinderrechte aus dem Blickwinkel der Digitalisierung«. In: *Schwerpunkt BILDUNGSverSUCHE* (2020), S. 20–23.

[20] Rebecca S Williams, K Jean Phillips-Weiner und Amy A Vincus. »Age verification and online sales of little cigars and cigarillos to minors«. In: *Tobacco regulatory science* 6.2 (2020), S. 152.