Thomas Kunz, Ulrich Waldmann*

Online-Altersverifikation zur Gewährleistung des Minderjährigenschutzes

Eine zuverlässige Altersverifikation ist für die Nutzung von Social-Media-Diensten erforderlich, wird aber oft nur unzureichend umgesetzt. Dies kann dazu führen, dass Minderjährige Dienste nutzen, die für ihr Alter ungeeignet sind. Dieser Beitrag untersucht die gängige Praxis der Altersverifikation und bewertet verschiedene Verfahren hinsichtlich ihrer Eignung. Demgegenüber gilt der Einsatz digitaler Identitäten wie Self-Sovereign Identity (SSI) als vielversprechender zukünftiger Lösungsansatz, der durch eIDAS 2 in Form von elektronischen Attributsbescheinigungen des European Digital Identity Wallet (EUDI-Wallet) unterstützt wird und eine datensparsame Alternative zur herkömmlichen Altersangabe ermöglicht.

1 Motivation

Social-Media-Dienste werden nicht nur von Erwachsenen genutzt, sondern in erheblichem Maße auch von Minderjährigen. Laut einer repräsentativen Studie im Auftrag des Digitalverbands Bitkom aus dem Jahr 2024[1] nutzen 93% der Kinder und Jugendlichen ab 10 Jahren soziale Netzwerke. Die durchschnittliche Nutzungsdauer der Kinder und Jugendlichen liegt bei 95 Minuten pro Tag. Allerdings sind nicht alle Social-Media-Dienste in gleichem Maße für alle Altersgruppen geeignet. So gibt es spezielle Dienste wie beispielsweise Dating-Apps, die sich explizit an Volljährige richten und bei denen sichergestellt werden muss, dass sie nicht von unter 18-Jährigen genutzt werden können. Generell ist zu beobachten, dass die meisten Social-Media-Dienste in ihren allgemeinen Geschäftsbedingungen ein Mindestalter von 13 Jahren für die Nutzung ihrer Dienste angeben.

Grundsätzlich kann davon ausgegangen werden, dass Social-Media-Dienste personenbezogene Daten verarbeiten und somit die DSGVO Anwendung findet. Als Rechtsgrundlage für die Verarbeitung kommt in erster Linie die Einwilligung in Frage. Die Erforderlichkeit der Datenverarbeitung für die Erfüllung eines Vertrags (Art. 6 Abs. 1 lit. b DSGVO) sowie die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (Art. 6 Abs. 1 lit. f DSGVO) kommen demgegenüber als Erlaubnistatbestände regelmäßig nicht oder allenfalls in ganz eingeschränktem Umfang in Betracht [2]. Im Falle Minderjähriger ist Art. 8 Abs. 1 DSGVO zu beachten. Demnach ist die Einwilligung des Kindes in die Verarbeitung personenbezogener Daten nur rechtmäßig, wenn das Kind das 16. Lebensjahr vollendet hat.[2] Bei Kindern unter 16 Jahren muss die Einwilligung entweder durch den Träger der elterlichen Verantwortung für das Kind oder mit dessen Zustimmung erteilt werden.

Dies macht es erforderlich, dass die Anbieter von Social-Media-Diensten das Alter zweifelsfrei feststellen müssen, um entschei-

* Das diesem Beitrag zugrunde liegende Vorhaben PriMeta wurde mit Mitteln des Bundesministeriums für Bildung und Forschung (BMBF) unter dem Förderkennzeichen 16KIS2050K gefördert. Diese Forschungsarbeiten wurden zusätzlich vom BMBF und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt. Die Verantwortung für den Inhalt liegt bei den Autoren.

Ulrich Waldmann

ist wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Sichere Informationstechnologie SIT und am Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE.
E-Mail: ulrich.waldmann@sit.fraunhofer.de

Thomas Kunz

ist wissenschaftlicher Mitarbeiter am Fraunhofer-Institut für Sichere Informationstechnologie SIT und am Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE.

E-Mail: thomas.kunz@sit.fraunhofer.de

1 https://www.bitkom.org/Presse/Presseinformation/Kinder-Jugendliche-taeglich-zwei-Stunden-Smartphone (zuletzt abgerufen am 16.01.2025)

2 Eine Öffnungsklausel in Art. 8 Abs. 1 DSGVO ermöglicht es den Mitgliedstaaten, die Altersgrenze auf 13 Jahre zu senken, in Deutschland wurde diese Möglichkeit jedoch bislang nicht angewandt.

den zu können, ob Nutzer selbst eine Einwilligung erteilen dürfen oder ob die Einwilligung der Eltern erforderlich ist. Hierbei ist es nicht ausreichend, dass Nutzer ihr vermeintliches Alter bei der Registrierung in ein Eingabefeld eingeben oder über einen Schalter angeben, mindestens 16 Jahre alt zu sein, denn dies würde dazu führen, dass die datenverarbeitende Stelle Daten von Minderjährigen verarbeiten könnte, ohne es zu wissen. Die DSGVO enthält allgemeine Nachweispflichten, mit denen sich die Notwendigkeit einer zweifelsfreien Ermittlung des Alters begründen lässt: Gemäß Art. 5 Abs. 2 DSGVO muss die datenverarbeitende Stelle als Verantwortlicher die Einhaltung datenschutzrechtlicher Grundsätze nachweisen und ist für die Rechtmäßigkeit der Datenverarbeitung verantwortlich. Entsprechend muss der Verantwortliche nach Art. 7 Abs. 1 DSGVO nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten (wirksam) eingewilligt hat, was bei nicht verifizierten Altersangaben möglicherweise wegen fehlender Einwilligungsfähigkeit nicht der Fall ist [2][11].

Neben dem Datenschutzrecht sind weitere gesetzliche Vorgaben bei Social-Media-Diensten relevant und machen eine Altersverifikation erforderlich. So regelt das Jugendschutzgesetz (§ 14 JuSchG) die Freigabe von Filmen und Spielen für Kinder und Jugendliche und definiert zu diesem Zweck fünf Kategorien (ohne Altersbeschränkung, freigegeben ab 6 Jahren, freigegeben ab 12 Jahren, Freigegeben ab 16 Jahren, keine Jugendfreigabe). Dies kann auch für bestimmte Social-Media-Dienste oder auch für Spieleplattformen relevant sein, die eine Mischform aus Spielen und sozialen Netzwerken darstellen.

Diese rechtlichen Anforderungen lassen sich durch die folgenden beiden grundlegenden Szenarien für eine Altersverifikation bei Social-Media-Diensten zusammenfassen.

1. **Altersverifikation aufgrund von Altersbeschränkungen.** Der Dienstanbieter muss das Alter prüfen, weil der Dienst ein bestimmtes Mindestalter voraussetzt, es geht also darum, bestimmte Altersgruppen von der Nutzung auszuschließen, zum Beispiel im Fall von Diensten, die nur von Volljährigen genutzt werden dürfen.
2. **Altersverifikation aufgrund der Notwendigkeit einer Einwilligung.** Bei Social-Media-Diensten, die auch von Minderjährigen genutzt werden dürfen, muss geprüft werden, ob ein Kind bereits 16 Jahre alt ist, da andernfalls die Eltern in die Erteilung einer Einwilligung in die Datenverarbeitung eingebunden werden müssen.

2 Beispiele aus der aktuellen Praxis

Bisherige Maßnahmen der Altersüberprüfung sind i. d. R. wenig innovativ und ermöglichen es insbesondere Minderjährigen, sehr einfach und auch ohne Einwilligung der Eltern ein Konto bei einem Social-Media-Dienst anzulegen.

Beispielsweise müssen Nutzer bei *WhatsApp* lediglich über eine Checkbox bestätigen, dass sie mindestens 13 Jahre alt sind, eine Überprüfung findet nicht statt. Bei *Facebook* und *Instagram* unterscheidet der Internetkonzern *Meta* grundsätzlich zwischen Nutzern unter 18 Jahren und Nutzern, die 18 Jahre oder älter sind. Letztere haben Zugriff auf zusätzliche Funktionen, die nur Erwachsenen vorbehalten sind. Um ein Konto für Nutzer unter 18 Jahre anzulegen, ist lediglich die Eingabe des Geburtsdatums erforderlich. Eine Einwilligung der Eltern ist nicht vorgesehen. 2022 hat *Meta* in den USA, inzwischen aber auch in weiteren Ländern, begonnen, für *Facebook* und *Instagram* weitere Optionen zur Altersüberprüfung einzuführen: Möchte ein Nutzer sein Alter auf „18 Jahre oder älter" ändern, stehen neben dem Hochladen von Ausweiskopien zwei weitere Optionen zur Verfügung. Bei der ersten Option erstellt die betroffene Person ein Video-Selfie, das an den Altersüberprüfungsdienst *Yoti* weitergeleitet wird.[3] Dort wird das Alter der betroffenen Person mittels KI-gestützter Gesichtsanalyse geschätzt und das Ergebnis an *Meta* übermittelt. Als Trainingsdaten verwendet *Yoti* pseudonymisierte Fotos von Jugendlichen und Erwachsenen aus der ganzen Welt.[4] Nach Angaben von *Meta* dient das aufgenommene Gesichtsbild keiner persönlichen Identifizierung und wird unmittelbar nach der Altersschätzung gelöscht. Die zweite Möglichkeit ist das so genannte „Social Vouching", bei dem die betroffene Person drei andere Personen über 18 Jahre auffordert, innerhalb von drei Tagen das von ihr angegebene Alter zu bestätigen.[5]

Im November 2024 kündigte *Meta* eine Verlagerung der Altersprüfung in App Stores oder Betriebssysteme an, um auf diese Weise eine einheitliche Altersverifikation zu erreichen, damit sich Dienste wie Facebook oder Instagram künftig nicht mehr um die Altersverifikation kümmern müssen. Zudem wird eine branchenweite Regelung gefordert, welche Inhalte für welche Altersgruppen als geeignet gelten – ähnlich wie es bei Filmen und Videospielen üblich ist. Darüber hinaus befürwortet *Meta* standardisierte Kontrolloptionen in Apps, die Eltern zum Schutz ihre Kinder aktivieren und konfigurieren können.[6]

Mit *Messenger Kids* bietet *Meta* einen Social-Media-Dienst für Minderjährige an. Hier können Kinder ihr Konto nicht selbst erstellen. Stattdessen nutzen die Eltern ihr Facebook-Konto, um für ihr Kind ein Konto anzulegen. Messenger Kids räumt den Eltern weitestgehende Kontrolle über die Aktivitäten ihrer Kinder ein. So können Kinder nur mit von den Eltern genehmigten Kontakten in Verbindung treten. Die Eltern können die Online-Aktivitäten ihres Kindes beobachten und beispielsweise Videos und Bilder entfernen oder melden, und einen weiteren Erziehungsberechtigten zum Konto des Kindes hinzufügen.[7]

TikTok führt bei der Registrierung keine Altersüberprüfung durch, kann aber bestehende Konten sperren, wenn Zweifel an der Einhaltung des Mindestalters von 13 Jahren bestehen. Prinzipiell können Minderjährige somit problemlos ohne Zustimmung der Eltern ein *TikTok*-Konto anlegen, zumal unklar ist, worauf sich die Zweifel stützen könnten. Nach einer Sperrung hat die betroffene Person 180 Tage Zeit, Einspruch zu erheben oder ihre Daten herunterzuladen. Abhängig von ihrem Wohnort können Jugendliche dann eine der drei folgenden Optionen nutzen, um ihr angegebenes Alter zwischen 13 und 17 Jahren zu bestätigen: 1) Hochladen eines Selfies, auf dem zusätzlich ein amtlicher Aus-

3 Meta: Ablauf der Altersverifizierung per Video-Selfie auf Facebook, https://de-de.facebook.com/help/1386337538619854/?helpref=related_articles

4 Yoti: Yoti Facial Age Estimation, White Paper, September 2024, https://www.yoti.com/wp-content/uploads/2024/11/Yoti-Age-Estimation-White-Paper-September-2024-PUBLIC.pdf

5 Instagram: Neue Möglichkeiten zur Altersverifizierung auf Instagram https://about.instagram.com/de-de/blog/announcements/new-ways-to-verify-age-on-instagram

6 Antigone Davis: Europe Can Make Parenting in a Digital World Easier, https://about.fb.com/news/2024/11/europe-can-make-parenting-in-a-digital-world-easier

7 Meta: Messenger Kids, https://www.facebook.com/help/messenger-app/213724335832452

weis und ein von *TikTok* zugesandter Code zu sehen sind. 2) Angabe der E-Mail-Adresse eines Erziehungsberechtigten, der dann von *TikTok* aufgefordert wird, das angegebene Alter des Jugendlichen zu bestätigen. 3) Hochladen eines Fotos, auf dem der Jugendliche zusammen mit einem Erziehungsberechtigten oder einer anderen vertrauenswürdigen Person im Alter von mindestens 25 Jahren zu sehen ist. Die erwachsene Person muss zudem ein Blatt Papier in der Hand halten, auf dem ein Altersnachweis, das Geburtsdatum des Jugendlichen und ein von TikTok generierter Code zu sehen sind.[8]

X setzt ebenfalls ohne Altersüberprüfung ein Mindestalter von 13 Jahren voraus und sperrt in Zweifelsfällen bestehende Konten. Somit können auch hier Minderjährige sehr einfach ohne Einwilligung der Eltern und ohne Nachweis ihres Alters ein Konto erstellen. Im Falle einer Kontosperrung muss die betroffene Person die Zustimmung eines Erziehungsberechtigten einholen, um das Konto wieder zu aktivieren. Dazu lädt der Erziehungsberechtigte über ein Online-Formular Kopien eines Ausweises und eines Nachweises der Erziehungsberechtigung (z. B. Geburtsurkunde) hoch.[9]

3 Verfahren der Altersprüfung

Die Verfahren zur Altersüberprüfung können in Altersangabe, Altersschätzung und Altersverifikation unterschieden werden [8]. Im Folgenden werden einige Verfahren hinsichtlich ihrer Wirksamkeit (d. h. der Zuverlässigkeit des Verfahrens), des Datenschutzes und der Praktikabilität untersucht.

- **Altersangabe**. Die betroffene Person wird online aufgefordert, ihr Geburtsdatum anzugeben oder zu bestätigen, dass ihr Alter über oder unter einer bestimmten Altersgrenze liegt. Dieses Verfahren ist weit verbreitet, aber am wenigsten zuverlässig, da keine Überprüfung der Angaben stattfindet. Das Verfahren kann jedoch dazu dienen, auf ungeeignete Dienste hinzuweisen. Das Verfahren kann datenschutzfreundlich gestaltet werden, wenn beispielsweise statt der Eingabe des vollständigen Geburtsdatums nur über einen Schalter ein bestimmtes Mindestalter bestätigt wird.
- **Altersschätzung mittels Verhaltensprofil**. Diese Verfahren nutzen Techniken der künstlichen Intelligenz, um aus den bisherigen Online-Aktivitäten auf das Alter der Person zu schließen. Die Schätzungen basieren beispielsweise auf identifizierten Interessen, Freunden und der besuchten Schule. Die Verfahren sind jedoch fehleranfällig und daher für viele Dienste ungeeignet. Als kontinuierlicher Prozess kann die Analyse von Verhaltensdaten (z. B. ausgetauschte Nachrichten) dazu dienen, festzustellen, ob eine minderjährige Person bei der Registrierung falsche Angaben über ihr Alter gemacht hat [9]. Der Umfang der Datenerhebung geht weit über den Zweck einer einfachen Altersschätzung hinaus.
- **Altersschätzung mittels Biometrie**. Verschiedene biometrische Verfahren wie Gesichtsanalyse, Handflächen- und Augenmessungen können zur Altersschätzung eingesetzt werden. Die Verfahren sind i. d. R. effektiv, bergen aber hohe Risiken für den Datenschutz der betroffenen Person. Eine Gesichtsanalyse muss zumindest nicht mit einer Gesichtserkennung verbunden sein, da für die Altersschätzung keine Identifizierung und Wiedererkennung der betroffenen Person erforderlich ist. Gegen Präsentationsangriffe mit vorgehaltenen Fotos, Masken oder Videos einer anderen (z. B. älteren) Person sind zudem Mechanismen der Lebenderkennung wichtig, beispielsweise die Aufforderung, den Kopf auf bestimmte Weise zu bewegen [6].
- **Altersverifikation mittels Kreditkarte**. Kreditkartenzahlung wird häufig bei Online-Käufen verwendet. Dazu muss die betreffende Person ihre Kreditkartendaten eingeben. Als Nebeneffekt lässt sich hierüber jedoch lediglich feststellen, dass die Person *wahrscheinlich* volljährig ist. Denn es ist nicht gewährleistet, dass tatsächlich der erwachsene Kreditkarteninhaber die Daten eingibt. Außerdem verfügen nicht alle Erwachsenen über eine Kreditkarte.
- **Altersverifikation mittels Ausweiskopie**. Hierbei wird die Person aufgefordert, ein offizielles Ausweisdokument einzuscannen und den Scan an den Anbieter zu senden, um das Alter bzw. eine Elternschaft zu bestätigen. Dabei werden meist zu viele personenbezogene Daten offengelegt. Zudem ist damit nicht nachgewiesen, dass der Ausweisinhaber tatsächlich anwesend und einverstanden ist. Kinder könnten z. B. leicht Kopien von Ausweisen ihrer Eltern oder älteren Geschwister anfertigen, um ein höheres Alter vorzutäuschen. Sie können zudem das eigene Geburtsdatum und Foto digital fälschen. Etwas mehr Sicherheit bietet der anschließende automatische Abgleich des Ausweisfotos mit einem Selfie-Foto der anwendenden Person durch den Dienstanbieter.
- **Altersverifikation mittels Videochat**. Über eine Webcam führt ein Mitarbeiter des Dienstanbieters oder ein KI-basierter Agent die zu überprüfende Person durch einen Videochat. Dabei wird die Person aufgefordert, ihren Personalausweis in die Kamera zu halten. Das Alter wird anhand des Geburtsdatums bestimmt, zudem wird das Foto mit dem Videobild der zu überprüfenden Person abgeglichen und es können die Sicherheitsmerkmale des Ausweises geprüft werden. Alternativ kann die Altersverifikation auch von einer unabhängigen dritten Partei durchgeführt werden, die das Ergebnis der Überprüfung an den Dienstleister weiterleitet (z. B. Person ist über 16 Jahre alt). Grundsätzlich werden aber auch bei diesem Verfahren i. d. R. zu viele personenbezogene Daten offengelegt. Denkbar sind auch Videochats mit Minderjährigen ohne Ausweis, in die auch die Eltern involviert werden. In diesem Fall wird der Videochat mit den Eltern durchgeführt, die sich mit ihrem Personalausweis identifizieren und das Alter ihres Kindes bestätigen.
- **Online-Ausweisfunktion**. Die Altersverifikation auf Basis von digitalen Identitäten wird von einigen Staaten wie z. B. Belgien, Frankreich und Deutschland unterstützt. Die Online-Ausweisfunktion des deutschen Personalausweises ist datenschutzfreundlich, da sie ausweis- und dienstspezifische Pseudonyme sowie Abfragen von Altersgrenzen unterstützt, ohne das genaue Geburtsdatum offenzulegen. Allerdings wird die Online-Ausweisfunktion bisher nur von wenigen Diensten unterstützt. Zudem kann die Funktion nur für Personen aktiviert und genutzt werden, die 16 Jahre und älter sind.
- **Self-Sovereign Identity (SSI)**. Bei SSI-basierten Verfahren stellen anerkannte und vertrauenswürdige Institutionen wie z. B. Meldebehörden („Issuer") für betroffene Personen digitale Identitätsdaten und Nachweise (z. B. Altersnachwei-

8 TikTok: Underage appeals on TikTok, https://support.tiktok.com/en/safety-hc/account-and-user-safety/underage-appeals-on-tiktok

9 X: About parental consent, https://help.x.com/en/using-x/parental-consent

se, Nachweise über die Elternschaft) in Form fälschungssicherer digital signierter Verifiable Credentials (VC) aus. VCs werden unter der Kontrolle der betroffenen Person („Holder") geschützt und dezentral in einem speziellen SSI-Wallet[10] i. d. R. auf dem Smartphone der Person, statt auf zentralen Servern, gespeichert. Die Person entscheidet somit darüber, welche VCs sie einem Dienst präsentiert und welche nicht. Das Ziel ist, dass dadurch ein Dienstanbieter nur die personenbezogenen Daten einer Person erhält, die für einen bestimmten Zweck absolut erforderlich sind (z. B. eine Altersangabe im Falle einer Altersverifikation). Hierbei ist es sogar möglich, mithilfe spezieller kryptografischer Verfahren, sog. „Zero-Knowledge Proofs", beispielsweise aus einem Nachweis über das Geburtsdatum eine verifizierbare Aussage wie „älter als 16 Jahre" abzuleiten und nur diese einem Dienstanbieter zu präsentieren. Der Dienstleister kann die Gültigkeit und Authentizität eines VC verifizieren („Verifier"). Die dafür benötigten öffentlichen Schlüssel sind in öffentlich zugänglichen Datenregistern (z. B. basierend auf Distributed Ledger Technologie) hinterlegt.

Tabelle 1 fasst die Bewertung der vorgestellten Verfahren zur Altersverifikation zusammen. Die Bewertungsskala reicht von „sehr gut" (++) über „mittel" (o) bis „sehr schlecht" (--). Nach wie vor sind die bloße Altersangabe und das Hochladen von Ausweiskopien gängige Praxis, schneiden aber insbesondere hinsichtlich der Wirksamkeit schlecht ab. Dies betrifft auch die Altersverifikation mittels Kreditkarte, zudem lässt sich hierbei nur feststellen, ob eine Person volljährig ist (vgl. Szenario 1 aus Kapitel 1). Für Minderjährige ist es ungeeignet, da diese über keine Kreditkarten verfügen.

Tabelle 1 | Bewertung der Verfahren

	Wirksamkeit	Datenschutz	Praktikabilität
Altersangabe	--	+	++
Verhaltensprofil	o	--	++
Biometrie	o	-	o
Kreditkarte	-	+	-
Ausweiskopie	-	-	+
Videochat	+	-	+
Online-Ausweisfunktion	++	++	o
Self-Sovereign Identity	++	++	+

Verfahren, bei denen das Alter lediglich geschätzt wird (Verhaltensprofil, Biometrie), sind insbesondere für die Umsetzung der in Kapitel 1 dargestellten Szenarien eher kritisch zu sehen, da nicht exakt ermittelt werden kann, ob beispielsweise ein bestimmtes Mindestalter erreicht ist. Eine KI-gestützte Altersschätzung anhand von Verhaltensprofilen oder biometrischen Merkmalen setzt zudem eine umfangreiche Erhebung personenbezogener Daten voraus, da genügend Verifikationsdaten des von der Schätzung Betroffenen als auch Referenzdaten (Trainingsdaten) anderer Personen zur Verfügung stehen müssen. Die Analyse von Verhaltensmerkmalen als Mittel zur Altersschätzung erscheint daher unverhältnismäßig. Für die Erhebung biometrischer Daten können zudem zusätzliche Geräte erforderlich sein, die über eine Webcam hinausgehen, und erscheinen daher nur wenig praktikabel. Videochats stellen ein wirksames und praktikables Verfahren zur Altersverifikation dar. Insbesondere wenn auch die Eltern in den Videochat eingebunden werden, ist das Verfahren gut dazu geeignet, das Alter von Minderjährigen mit Einwilligung der Eltern zu bestimmen. Bezüglich des Datenschutzes schneiden Videochats jedoch weniger gut ab, da für eine reine Altersverifikation zu viele personenbezogene Daten erhoben werden (Ausweisdaten, Videobild der teilnehmenden Personen).

Hinsichtlich Wirksamkeit und Datenschutz liefern die Online-Ausweisfunktion und SSI-basierte Verfahren die besten Ergebnisse. Die Online-Ausweisfunktion ist in Deutschland mit der Smartphone-tauglichen AusweisApp[11] zwar praxistauglicher geworden, wird aber nach wie vor nur von wenigen Diensten unterstützt. Zudem ist sie nur bedingt für die Umsetzung der Szenarien aus Kapitel 1 geeignet, da Kinder unter 16 Jahren in Deutschland nur Personalausweise ohne Online-Ausweisfunktion ausgestellt bekommen. Am vielversprechendsten erscheint daher ein europaweites SSI-basiertes Verfahren der Altersverifikation. Dabei werden VCs in digitalen Wallets auf dem Smartphone gespeichert. Da heutzutage auch unter 16-Jährige i. d. R. über ein eigenes Smartphone verfügen und Wallet-Apps bereits in anderen Kontexten (z. B. für Tickets) nutzen, könnten zukünftig mittels SSI die Szenarien der Altersverifikation gut umgesetzt werden. Das nachfolgende Kapitel 4 geht daher ausführlicher auf die besonderen Herausforderungen bei der Umsetzung dieser Verfahren ein.

4 SSI-basierte Altersverifikation

Wie im vorangegangenen Kapitel dargelegt, bieten SSI-basierte Verfahren große Vorteile hinsichtlich des Datenschutzes (insb. Datenminimierung) und der informationellen Selbstbestimmung. Die Umsetzung von SSI-basierten Verfahren ist jedoch auch mit einigen Herausforderungen verbunden, die im Folgenden diskutiert werden.

Eine Grundvoraussetzung für die Nutzbarkeit digitaler Identitäten und Nachweise ist Interoperabilität. Möglichst viele Dienste müssen solche Nachweise akzeptieren. Dies wird u. a. durch Standardisierung erreicht: Die benötigten Datenformate und Mechanismen werden durch das World Wide Web Consortium (W3C) spezifiziert [14][15]. Zudem muss die benötigte Infrastruktur bereitgestellt werden. Dies betrifft insbesondere die Verfügbarkeit öffentlicher Datenregister.

Die benötigten SSI-Wallets müssen über eine hohe Sicherheit verfügen, da in ihnen beliebige personenbezogene Daten einer Person gespeichert werden und somit ein attraktives Ziel für Angreifer darstellen [10].

Eine wichtige Basis für SSI stellen dezentrale IDs (Decentralized Identifier, DID) dar [15]. Diese sind jeweils einer Person bzw. Institution zugeordnet, referenzieren jeweils ein Schlüsselpaar und sind fester Bestandteil der VCs. Jede Person kann beliebig viele DIDs besitzen. Bei der Präsentation eines VC gegenüber einem Dienst muss die betroffene Person somit nicht mit immer dem gleichen DID in Erscheinung treten. Dadurch soll die Rückführbarkeit mehrerer VC zu einer Person durch einen Dienst

10 European Blockchain Association: SSI Wallets, https://europeanblockchainassociation.org/ssi-wallets/

11 Governikus: https://www.ausweisapp.bund.de/online-ausweisfunktion-nutzen

und damit die Profilbildung erschwert werden. Vollständig verhindern lässt sich eine Profilbildung jedoch nicht, insbesondere nicht, wenn ein Dienst mehrere Merkmale einer Person abfragt oder wenn Dienste miteinander kooperieren und VCs ihrer Nutzer untereinander austauschen [10]. Zu bedenken ist in diesem Zusammenhang auch, dass verifizierte Identitätsdaten wertvoller für den Handel oder Missbrauch sein können. Eine unbefugte Sammlung, Verknüpfung und Weitergabe verifizierter Daten durch die Dienstanbieter kann somit nicht komplett verhindert werden, wodurch betroffene Personen die Hoheit über ihre Daten wieder verlieren können [1]. Identifizierungspflichten im Internet könnten durch eine SSI-Infrastruktur vereinfacht und damit auch politisch leichter durchsetzbar werden.[12] Zudem könnten ausufernde Identifizierungspflichten an staatliche und gesellschaftliche Privilegien geknüpft werden [16].

Daher sind strenge rechtliche Rahmenbedingungen erforderlich. Wesentlich ist die Gestaltung eines angemessenen SSI-Vertrauensmodells, nach dem die Verifizierer den (ihnen i. d. R. unbekannten) Issuern vertrauen können. Um ein hohes Maß an Sicherheit zu erreichen, können zusätzlich zu Blockchain-basierten DIDs zentrale Instanzen als Vertrauensanker mittels einer klassischen PKI etabliert werden [1], siehe europäische *Trusted Lists* im nächsten Kapitel.

5 Möglichkeit der EU-weiten Einführung

Die eIDAS-Verordnung von 2014 unterstützt zwar die Online-Ausweisfunktion und die Authentifizierung von digitalen Dokumenten, hat aber die erhoffte Verbreitung von digitalen Identitäten nicht erreichen können.[13] Einheitliche SSI-basierte Lösungen erfordern eine rechtliche Grundlage für neue organisatorische und technische Infrastrukturen wie die im Aufbau befindliche *European Blockchain Service Infrastructure* (EBSI) [7][13].

Mit der 2024 erfolgten Novellierung und Erweiterung der eIDAS-Verordnung („eIDAS 2“) [4] werden nun digitale Identitätsnachweise und elektronische Attributsbescheinigungen auf Basis von SSI und Blockchain ausdrücklich unterstützt. Art. 5a und Art. 45b-h eIDAS 2 sehen für jeden EU-Bürger die Einrichtung eines *European Digital Identity Wallets* („EUDI-Wallet“) mit Unterstützung von elektronischen Attributsbescheinigungen vor.

12 Wittmann, L.: Mit dem Personalausweis zum Onlineshopping: Wie selbstbestimmt sind „selbstbestimmte Identitäten“? https://lilithwittmann.medium.com/mit-dem-personalausweis-zum-onlineshopping-wie-selbstbestimmt-sind-selbstbestimmte-identitäten-f096a5bdd55a

13 BMI: Die eIDAS-Verordnung, EUDI-Wallets und ihre Bedeutung für europäische digitale Identitäten, https://www.digitale-verwaltung.de/Webs/DV/DE/digitale-identitaeten/eidas-2-0/eidas-2-0.html

Zukünftige Anbieter sollen mit ihren kryptografisch überprüfbaren Vertrauensankern in die bestehenden *Electronic Signatures and Infrastructures (ESI) Trusted Lists* aufgenommen werden [5][7].

Die eIDAS Expert Group der Europäischen Kommission hat ein erstes Framework für die europäische digitale Identität erstellt [3]. Die technischen Details des EUDI-Wallets werden zurzeit bei ETSI und CEN spezifiziert [5], die Einführung soll von mehreren Pilotprojekten begleitet werden [12]. In Deutschland erarbeitet zurzeit ein Expertenteam unter Federführung des BMI einen Architekturvorschlag für das EUDI-Wallet.[14] Darin sind folgende Altersgrenzen für die Altersverifikation vorgesehen: „gleich oder älter" 12, 14, 16, 18, 21 und 65 Jahre. Auf europäischer Ebene werden Durchführungsrechtsakte mit Listen der technischen Normen, Einrichtung von Konformitätsbewertungsstellen und die Entwicklung von Referenzimplementierungen folgen. Gemäß Art. 5a eIDAS 2 haben die Mitgliedstaaten nach Inkrafttreten der Durchführungsrechtsakte zwei Jahre Zeit (bis Ende 2026), um das EUDI-Wallet mit Unterstützung der in Anhang VI eIDAS 2 festgelegten Mindestliste von Attributen (einschließlich „Alter" und „Familienzusammensetzung") bereitzustellen.

6 Fazit

Social-Media-Dienste bleiben bei der Altersprüfung meist weit hinter den rechtlich geboten Maßnahmen und technischen Möglichkeiten zurück. Die Altersverifikation sollte nicht allein den großen Internetunternehmen überlassen werden. Eine einheitliche Lösung kann das zukünftige EUDI-Wallet mit der Möglichkeit von SSI-basierten Attributsbescheinigungen u. a. des Alters und der Familienzusammensetzung bieten. Dabei spielen Vertrauensmechanismen eine entscheidende Rolle. Sie müssen einheitlich sein und ein höheres Maß an Gewissheit bieten, als dies bei den heute gängigen Verfahren der Fall ist.

Das SSI-basierte EUDI-Wallet und die Online-Ausweisfunktion sind keine echten Konkurrenten. Denn das EUDI-Wallet wird die gleichen staatlich geprüften Daten enthalten, allerdings in signierter Form. Wichtig ist, dass die nach Art. 5a (14) und Art. 45h eIDAS 2 für Anbieter von Wallets und Attributsbescheinigungen unzulässige Verknüpfung personenbezogener Daten mit Daten anderer Dienste wirksam kontrolliert wird, damit keine neuen, zentralen Datensammlungen entstehen. Darüber hinaus kann die Datenminimierung auch dadurch gefördert werden, dass festgelegt wird, welche Daten für welche Zwecke abgefragt werden dürfen. Dann besteht die Aussicht, dass durch das EUDI-Wallet eine praktikable und europaweit einheitliche Lösung für die Altersverifikation zur Verfügung steht. Bei einer Einführung des EUDI-Wallets bis Ende 2026 ist mit einer flächendeckenden Unterstützung durch die Dienstanbieter frühestens ab 2030 zu rechnen.

14 BMI: eIDAS 2.0 Architecture Concept, https://gitlab.opencode.de/bmi/eudi-wallet/eidas-2.0-architekturkonzept/

Literatur

[1] Eckpunktepapier für Self-sovereign Identities (SSI) unter besonderer Berücksichtigung der Distributed-Ledger-Technologie (DLT). Bundesamt für Sicherheit in der Informationstechnik, 2021.

[2] Buchner, B.: Der Schutz von Minderjährigen in der Datenökonomie – Die Meta-Entscheidung des EuGH und der Minderjährigendatenschutz. Datenschutz und Datensicherheit, Vol. 47, 2023.

[3] European Commission's eIDAS Expert Group: The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework – The European Digital Identity Wallet, Architecture and Reference Framework. Version 1.0.0, 2023.

[4] European Union: Verordnung (EU) 2024/1183 des Europäischen Parlaments und des Rates vom 11. April 2024 zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung des europäischen Rahmens für eine digitale Identität, 2024.

[5] ETSI TR 119 476 V1.2.1: Electronic Signatures and Trust Infrastructures (ESI); Analysis of selective disclosure and zero-knowledge proofs applied to Electronic Attestation of Attributes, 2024.

[6] Freiberg, A. K.: Lebenderkennung – Schutz für die biometrische Identität. Datenschutz und Datensicherheit, Vol. 47, 2023.

[7] Kudra, A., Seegebart, C., Schwalm, S. (2022). "Ein digitaler Vertrauensraum für Identitäten und Dienste – Europa ist auf dem richtigen Weg: Ein Impuls". Datenschutz und Datensicherheit, Vol. 46, 2022.

[8] ITU Focus Group on Metaverse: Children's age verification in the metaverse. International Telecommunication Union, 2023.

[9] Pasquale, L. u. a.: Digital age of consent and age verification – Can they protect children? IEEE Software 39.3, S. 50–57, 2020.

[10] Sas, M., Mühlberg, J. T.: Trustworthy Age Assurance? A risk-based evaluation of available and upcoming age assurance technologies from a fundamental rights perspective. The Greens/EFA Group at the European parliament, 2024.

[11] Schnebbe, M.: Minderjährigenschutz in der DS-GVO. Datenschutz und Datensicherheit, Vol. 46, 2022.

[12] Schwalm, S.: The possible impacts of the eIDAS 2.0 digital identity approach in Germany and Europe. Gesellschaft für Informatik, 2023.

[13] Schwalm, S., Mueller, K.: Qualifizierte Ledger – der Durchbruch für Blockchain: Geprüfte Sicherheit und rechtliches Vertrauen mit eIDAS 2.0? Datenschutz und Datensicherheit, Vol. 48, 2024.

[14] W3C Recommendation: Verifiable Credentials Data Model v1.1. World Wide Web Consortium (W3C), 2022.

[15] W3C Recommendation: Decentralized Identifiers (DIDs) v1.0 – Core architecture, data model, and representations. World Wide Web Consortium (W3C), 2022.

[16] Weigl, L. u. a.: The social construction of self-sovereign identity: An extended model of interpretive flexibility. Proceedings of the 55th Hawaii International Conference on System Sciences, 2022.