

Dokumentation

WS II „Datensparsame Altersverifikation“

Donnerstag, 6. Juli 2023

BMFSFJ, Schöneberger Ufer 75, 10785 Berlin

1 Ausgangslage

1.1 Aktuelles zum Verordnungsentwurf zur Prävention und Bekämpfung des sexuellen Missbrauchs der Europäischen Kommission (CSA-R)

Eine Altersverifikation für alle Nutzenden kann ein wesentliches Element zur Schaffung sicherer Räume im digitalen Umfeld sein. Ziel ist ein Konzept für ein datensparsames Verfahren, welches ein hohes Maß an Anonymität gewährleistet.

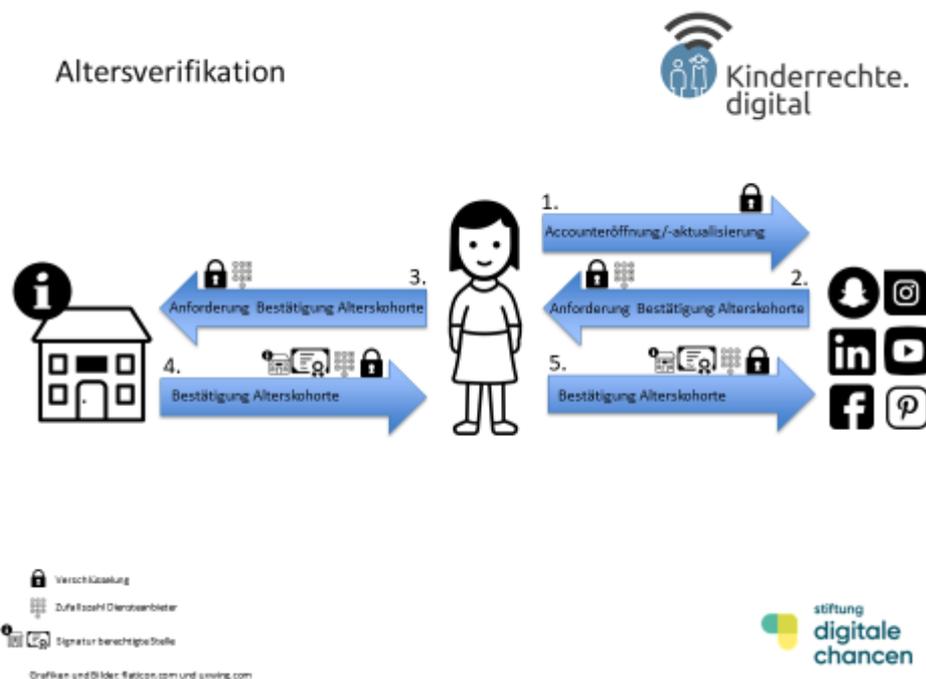
In der deutschen Stellungnahme zum Entwurf der CSA-R wird u.a. betont, dass bestehende Verschlüsselungssysteme von Kommunikationsinhalten Bestand haben sollen und dass sich die Bundesregierung aktiv in die Entwicklung eines europaweit einsetzbaren Altersverifikationssystems einbringen wird. Altersverifikation wird im Kontext der CSA-R als eine Maßnahme zur Risikominderung erachtet. Sie soll daher dort zur Anwendung kommen, wo dies effektiv zur Minderung eines Risikos beitragen kann. Für Nutzende digitaler Dienste soll eine Auswahl verschiedener Verfahren zur Verfügung stehen. Sofern Nutzende eines risikobehafteten Dienstes sich einem Altersverifikationsverfahren nicht unterziehen möchten, wird ihnen dieser in der sichersten möglichen Voreinstellung angeboten werden.

Aktuell strebt die spanische Ratspräsidentschaft eine Positionierung der Regierungen der Mitgliedsstaaten zur CSA-R bis Ende September 2023 an.

1.2 Rückblick auf den Workshop I vom 29. März 2023

Der Ausgangsvorschlag für ein Verfahren zur Altersverifikation basierend auf einer permanenten ID sowie einer neutralen dritten Stelle, welche die notwendige Verifikation vornimmt, wurde am 29. März 2023 umfassend diskutiert. Die aus dem Kreis der Teilnehmenden gegebenen zahlreichen Hinweise, Nachfragen und Anregungen flossen anschließend in die Weiterentwicklung des Ansatzes ein. Dabei wurden Aspekte der benötigten Daten sowie deren Umfang, die Wahrung von Anonymität, der möglichen Bildung von Profilen, von Inklusion und Zugänglichkeit, Verlässlichkeit sowie Präzision, der Rolle von Eltern und anderen Betreuungs- und Erziehungspersonen sowie hinsichtlich der Notwendigkeit aller Nutzenden, ihr Alter zu verifizieren, berücksichtigt. (vgl. dazu auch Dokumentation WS „Datensparsame Altersverifikation“ vom 29. März 2023).

2 Vorstellung und Erörterung des weiterentwickelten Konzepts zur Altersverifikation



Anhand eines Schaubildes (s. Anlage 1) wurde das weiterentwickelte Konzept erläutert. Demnach werden Nutzende eines Services bei der Eröffnung eines Accounts bzw. dessen Aktualisierung – sofern vor dem Hintergrund bestehender Risiken notwendig – durch den Anbieter des Dienstes aufgefordert, sich mittels Verifikation einer Alterskohorte zuzuordnen, damit für Minderjährige ihrer jeweiligen Kohorte entsprechende Vorsorgeeinstellungen und Sicherungsmaßnahmen angeboten werden können, während für Volljährige i.d.R. der volle Funktionsumfang bereitgestellt wird. Damit der Nachweis der korrekten Alterskohorte erbracht werden kann, übergibt der Diensteanbieter der nutzenden Person automatisiert eine Zufallszahl, die es anschließend ermöglicht, den Nachweis dem korrekten Account zuzuordnen zu können, ohne Kenntnis über die nutzende Person zu erlangen. Diese Zufallszahl wird mit der Anforderung der Zuordnung zu einer Alterskohorte an eine zur Verifikation berechtigte Stelle übermittelt. Diese erfährt nicht, für welchen Dienst der Nachweis geführt wird, sondern bestätigt ausschließlich der nutzenden Person auf der Grundlage der bei ihr gespeicherten Daten die Zugehörigkeit zu einer Alterskohorte. Dafür wird die zuvor übermittelte Zufallszahl mit einer entsprechenden Signatur versehen und anschließend durch die nutzende Person an den Diensteanbieter weitergereicht. Dieser erkennt anhand der Zufallszahl die Zuordnung zum gewählten Account und anhand der Signatur, dass eine berechtigte Stelle die Zugehörigkeit zu einer Alterskohorte bestätigt hat. Eine Information darüber, welche Stelle den Nachweis geführt hat, erhält der Diensteanbieter nicht.

In der Erörterung des weiterentwickelten Konzepts standen technische Aspekte im Vordergrund. Nachgefragt wurde aber auch, wie sich Eltern oder andere Erziehungspersonen in dieses Verfahren einbringen können bzw. sollten.

Tabelle 1: Darstellungen von nachgefragten Themen und diskutierten Lösungsansätzen

<ul style="list-style-type: none"> Übermittlung des bestätigten Altersnachweises <i>Wie gelangt der bestätigte Altersnachweis von der berechtigten Stelle zum Diensteanbietenden?</i> 	<p>Das Verfahren kann theoretisch auf verschiedenen Wegen durchlaufen werden (postalisch, E-Mail). Um eine hohe Usability und Akzeptanz seitens der Nutzenden zu erreichen, erscheint ein Verifikationsprozess über eine Browserextension sinnvoll.</p>
<ul style="list-style-type: none"> Weitergabe des bestätigten Altersnachweises <i>Ist der bestätigte Altersnachweis vor unberechtigter Weitergabe geschützt?</i> 	<p>Der bestätigte Altersnachweis kann theoretisch an Dritte weitergereicht werden. Um dem entgegenzuwirken, kommen eine zeitliche Limitierung der Gültigkeit beim Datenaustausch auf ein für die technische Umsetzung notwendiges Zeitfenster sowie wiederholte Nachweisanforderungen in unbekanntem Zeitabständen in Frage.</p>
<ul style="list-style-type: none"> Aktualisierung des Accounts <i>Woher weiß der Dienst, wann ein Account hinsichtlich der Alterskohorte aktualisiert werden muss? Ist dafür die Kenntnis des Geburtsdatums notwendig?</i> 	<p>Der Dienst kennt das Geburtsdatum der nutzenden Person nicht und kann daher die Aktualisierung des Accounts, wenn der Übergang in eine neue Alterskohorte erreicht wird, nicht anstoßen. Der Aktualisierungsimpuls geht von der nutzenden Person aus. Dabei ist davon auszugehen, dass diese im Eigeninteresse, bspw. um einen größeren Nutzungs- und Berechtigungsumfang zu erreichen, mit dem Wechsel in eine neue Alterskohorte die Aktualisierung anstoßen wird. Unabhängig davon kann die Accountaktualisierung auch mittels der wiederholten Nachweisanforderung zu einem unbekanntem Zeitpunkt erfolgen.</p>
<ul style="list-style-type: none"> Anmeldeverfahren/ Nutzungsverfahren <i>Wie kann während der laufenden Nutzung (session) hinsichtlich der Zuordnung zur Alterskohorte Sicherheit gewährleistet werden?</i> 	<p>Während der laufenden Nutzung (session) kann die Zuordnung zur korrekten Alterskohorte mittels eines mitgeführten Merkmals, bspw. gesichertes Cookie, nachgewiesen werden.</p>
<ul style="list-style-type: none"> Kenntnis der signierenden Stelle <i>Erfährt der Dienst, welche Stelle die Alterskohorte verifiziert hat?</i> 	<p>Nein, der Dienst erfährt lediglich, ob die Stelle zur Altersverifikation berechtigt ist und welcher Alterskohorte die nutzende Person angehört. Der Dienst erlangt keine Kenntnis darüber, welche Stelle das Alter verifiziert. Ebenso kann die verifizierende Stelle nicht erkennen, für welchen Dienst die Altersverifikation der Person durchgeführt wird.</p>

<ul style="list-style-type: none"> • Mobile Anwendungen <i>Funktioniert das Verfahren der Browsererweiterung (Browserextension) auch bei Apps?</i> 	<p>Ja, das Verfahren kann auch bei Apps angewandt werden.</p>
<ul style="list-style-type: none"> • Authentifizierung der Person <i>Woher weiß die signierende Stelle, welche Person um Altersverifizierung nachfragt?</i> 	<p>Die Person muss sich bei Übergabe der Zufallszahl sowie der Altersverifikationsanforderung authentifizieren, bspw. mittels bestehender Login-Verfahren. Vorstellbar ist auch, dass ein entsprechendes persönliches Zertifikat direkt in die Browserextension implementiert wird.</p>
<ul style="list-style-type: none"> • Verschiedene Endgeräte <i>Wie wird das Verfahren bei Nutzung verschiedener Endgeräte sichergestellt? Wie wird der unberechtigte Zugriff Dritter bei geteilter Nutzung von Endgeräten gewährleistet?</i> 	<p>Sicherheit kann über individuelle Accounts, welche jeweils altersverifiziert sind, erreicht werden. Darüber hinaus kann unabhängig vom Endgerät zu zuvor nicht bekannten Zeitpunkten eine erneute Altersverifikation durchgeführt werden.</p>
<ul style="list-style-type: none"> • Non-EU Dienste <i>Wie können Diensteanbieter, welche außerhalb der Europäischen Union ihren Sitz haben, zur Teilnahme am Altersverifikationsverfahren motiviert werden?</i> 	<p>Die CSA-R verpflichtet auch Anbieter, die ihren Sitz nicht in der Europäischen Union haben, zur Anwendung von Schutzeinstellungen und Vorsorgemaßnahmen, wenn sie ihren Dienst in der Europäischen Union anbieten.</p>
<ul style="list-style-type: none"> • Juristische Absicherung technischer Lücken 	<p>Technische Systeme können generell keine 100-prozentige Sicherheit gewährleisten, eine rechtliche Absicherung ist angeraten.</p>
<ul style="list-style-type: none"> • Erzieherische Illusion des Schutzraumes <i>Suggestieren altersverifizierte Angebote mehr Sicherheit als diese zu leisten vermögen?</i> 	<p>Durch Altersverifikation aller Nutzenden können Risiken minimiert und eine höhere Sicherheit für Minderjährige erreicht werden, als dies bisher der Fall ist. Die medienerzieherische Begleitung durch Eltern und andere Betreuungspersonen bleibt weiterhin erforderlich, darf jedoch nicht für alle Minderjährigen als selbstverständlich angenommen werden.</p>

<ul style="list-style-type: none"> • Kompetenz der Eltern („Erziehungsoffenheit“) <i>Wie ordnet sich die Kompetenz der Eltern in das Konzept der Altersverifikation ein? Wie können deren Erziehungsrechte Berücksichtigung finden?</i> 	<p>Diese Frage konnte im Workshop nicht abschließend geklärt werden. Erörtert wurde, ob in das Verfahren der Altersverifikation eine Beteiligungsoption oder gar ein Erlaubnisvorbehalt der Eltern zu implementieren wäre. Darüber hinaus wurde eine Einbindung/Anknüpfung an bestehende Systeme der elterlichen Begleitung (parental control) erwogen.</p>
<ul style="list-style-type: none"> • Fähigkeit des Kindes <i>Sind bzw. ab wann sind Kinder in der Lage, das Altersverifikationsverfahren selbständig durchzuführen?</i> 	<p>Im Fokus des Interesses stehen Account gebundene Anwendungen, bspw. bei Social Media Diensten. Für Kinder, die in der Lage sind, eigene Konten/Profile zu erstellen und zu pflegen, kann davon ausgegangen werden, dass sie auch das Login-Verfahren für die Authentifizierung während des Verifikationsverfahrens bewältigen können, insbesondere wenn dieses über eine Extension gelöst wird.</p>
<ul style="list-style-type: none"> • Einstellungserhalt bei Accountaktualisierung <i>Angeregt wurde, dass auch bei Aufwachsen in eine ältere Alterskohorte die Möglichkeit bestehen sollte, die höheren Schutzeinstellungen bzw. Vorsorgemaßnahmen der jüngeren Kohorte beibehalten zu können</i> 	<p>Der Erhalt der Einstellungen sowie deren individuelle (Neu-)Einrichtung muss durch die Gestaltung der Anwendung durch die Diensteanbieter gewährleistet werden.</p>
<ul style="list-style-type: none"> • Kinder als Täter:in <i>Hingewiesen wurde darauf, dass ein solches Verfahren Schutz vor möglichen älteren Täter:innen gewährt, jedoch nicht vor Täter:innen in derselben Alterskohorte.</i> 	<p>Das System soll zusätzlichen Schutz ermöglichen und bestehende bzw. alternative Schutz- und Vorsorgemaßnahmen nicht ersetzen. Moderation in Kommunikationsräumen, Medienerziehung, Meldedfunktionen, etc. können Sicherheit zwischen Menschen innerhalb einer Alterskohorte ermöglichen.</p>
<ul style="list-style-type: none"> • Aufgabe des Nutzenden <i>Was kommt konkret auf die Nutzenden zu? Was haben sie zu tun?</i> 	<p>Eine Browserextension erleichtert Verfahren der Altersverifikation erheblich. Die Nutzenden müssen sich für eine der zur Altersverifikation berechtigten Stellen entscheiden und sich gegenüber dieser als Person authentifizieren.</p>
<ul style="list-style-type: none"> • Personalausweis/ eIDs <i>Angeregt wurde die eID-Funktion des Personalausweises zu berücksichtigen.</i> 	<p>Die eID-Funktion des Personalausweises steht derzeit ab 16 Jahren zur Verfügung und kann zur Altersverifikation genutzt werden (Wahlfreiheit).</p>

<ul style="list-style-type: none"> • single-sign-on <i>Angeregt wurde Verfahren zur einmaligen Nachweisführung zu etablieren und zu ermöglichen, dass verifizierte Accounts bei Neuanmeldungen/Aktualisierungen zur Anwendung kommen können.</i> 	<p>Die Option eines single-sign-on wurde im Rahmen des euConsent-Projektes erprobt; ein fachlicher Austausch hat bereits stattgefunden, weitere Möglichkeiten der Zusammenarbeit werden geprüft.</p>
---	--

3 Anonyme Altersverifikation für alle Nutzer*innen

Zur Gewährleistung des Rechts auf informationelle Selbstbestimmung für alle Nutzenden sollte Altersverifikation nur für Dienste verpflichtend sein, für die im Zuge einer Risikobewertung erhebliche Risiken in Bezug auf die Verbreitung von Darstellungen der sexuellen Gewalt gegenüber Minderjährigen sowie des Groomings festgestellt wurden. Eine Nutzung des jeweiligen Dienstes ohne vorherige Durchführung des Altersverifikationsprozesses soll in einem durch entsprechende Voreinstellungen abgesicherten Modus möglich sein. Für alle nutzenden Personen soll eine große Auswahl verschiedener Verfahren der Altersverifikation angeboten werden.

Das zu entwickelnde Modell soll perspektivisch als datensparsames und anonymes Verfahren neben die bestehenden und zertifizierten Altersverifikationsverfahren treten. Die Entscheidung für ein Verfahren wird von der nutzenden Person individuell getroffen.

Als Verifizierungsstelle kommen aus Gründen der Datensparsamkeit Einrichtungen in Betracht, die bereits über die notwendigen Daten der Nutzenden verfügen. Es ist nicht vorgesehen, dass für die Altersverifikation Daten neu erhoben oder nachgewiesen werden müssen. Bemerkt wurde, dass vor dem Hintergrund der Akzeptanz und mit Blick auf die anstehende politische Kommunikation nicht (ausschließlich) auf staatliche Einrichtungen abgestellt werden sollte. Ein mögliches Narrativ, wonach staatliche Stellen über die Zugänglichkeit zu digitalen Diensten entscheiden würden, könnte für die Realisierung des Vorhabens kontraproduktiv sein. Ebenso müsse gewährleistet werden, dass die berechtigten Stellen keine Profilbildung hinsichtlich digitaler Aktivitäten führen können. Dies wird dadurch ausgeschlossen, dass die verifizierenden Stellen grundsätzlich anhand der Zufallszahl keine Kenntnis darüber erlangen, für welchen Dienst der Nachweis der Zugehörigkeit zu einer Alterskohorte geführt wird.

Als mögliche Stellen für eine Altersverifikation kommen u.a. grundsätzlich in Betracht:

- Melderegister
- Banken
- Krankenkassen
- Kraftfahrtbundesamt

Angeregt wurde auch darüber nachzudenken, ob nicht auch Eltern als entsprechende Nachweis führende Stelle in Betracht kommen. Dies wurde mit dem Anspruch an deren Verantwortung für die Medienerziehung ihrer Kinder sowie mit ihrem Erziehungsvorrang und auch ihrem ggf. notwendigen Einwilligungsvorbehalt hinsichtlich der Datenverarbeitung begründet.

Ebenso wurde auf bestehende Prozesse zur Realisierung der Maßnahmen im Rahmen der Umsetzung des Onlinezugangsgesetzes verwiesen und angeregt, Querverbindung und mögliche Potenziale zu prüfen.

4 Ausblick und Verabschiedung

Alle Teilnehmenden erhalten im Nachgang der Beratung eine Dokumentation des Workshops. Soweit erforderlich wird es weiteren bilateralen Austausch geben, eine weitere Beratung im Workshopformat ist vorerst nicht geplant.

Die Anregungen aus der Beratung und die aufgeworfenen Aspekte werden im Hinblick auf die Weiterentwicklung und Präzisierung des vorgestellten Konzeptes berücksichtigt. Anschließend ist vorgesehen, das Konzept in eine Verständigung im Ressortkreis einzubringen und infolgedessen in die weiteren Beratungen der CSA-R einfließen zu lassen.

Anhang Erläuterung Browser- / App-Extension

Eine Extension für gängige Webbrowser oder Apps auf mobilen Endgeräten kann hierbei Teile des Verifikationsprozesses automatisieren und der nutzenden Person, von der eine Altersverifikation angefordert wird, so bspw. mit folgenden denkbaren Schritten unterstützen:

1. Die Browserextension reagiert zunächst auf eine initiale Anfrage eines Diensteanbieters nach einer Altersverifikation: Sie zeigt der nutzenden Person ein Fenster mit dem Hinweis an, dass eine Altersverifikation gefordert wird und erfragt, ob diese durchgeführt werden soll.
2. Bestätigt die nutzende Person, dass eine Altersverifikation durchgeführt werden darf, nimmt die Browserextension automatisch eine Zufallszahl des Diensteanbieters entgegen, die dieser erzeugt und mit der nutzenden Person assoziiert hat, sowie die konkrete Anfrage des Dienstes zur Alterskohorte (bspw. "Ist die Person mind. 16 Jahre alt?").
3. Die Browserextension reicht diese Anfrage zusammen mit der Zufallszahl automatisch an eine berechnete Stelle weiter, die die nutzende Person entweder interaktiv auswählt oder im Voraus bereits festgelegt und in der Browserextension hinterlegt hat.
4. Die berechnete Stelle nimmt Zufallszahl und Frage nach Alterskohorte entgegen und fordert dabei die Authentifizierung der nutzenden Person. Diese kann sich bspw. mit zuvor erhaltenen Zugangsdaten oder einem persönlichen Zertifikat authentifizieren. Neben einer interaktiven Authentifizierung ist ebenfalls denkbar, vorab die Authentifizierungsinformationen (also Zugangsdaten, persönliches Zertifikat, o.ä.) in der Browserextension zu hinterlegen, sodass keine Interaktion durch die nutzende Person notwendig ist.
5. Nach erfolgreicher Authentifizierung bei der berechneten Stelle kann diese die Zugehörigkeit zur angefragten Alterskohorte bestätigen, indem sie eine entsprechende Aussage dazu mitsamt der vom Diensteanbieter erstellten Zufallszahl digital signiert.
6. Die Browserextension nimmt diese signierte Antwort, die die Aussage zur Zugehörigkeit der angefragten Alterskohorte sowie die Zufallszahl enthält, automatisch entgegen und leitet sie an den Diensteanbieter weiter.

7. Der Diensteanbieter kann nun anhand der digitalen Signatur überprüfen, ob die nutzende Person der angefragten Alterskohorte zugehört und ob die Stelle, die die digitale Signatur erstellt hat, dazu berechtigt ist. Ist beides der Fall, so ist die Zugehörigkeit der Alterskohorte der nutzenden Person gegenüber dem Diensteanbieter verifiziert und der Diensteanbieter kann nun auf dieser Basis den Zugang zu entsprechenden Medien gewähren.

5 **Teilnehmende**

- [REDACTED], Universität Mainz (*zeitweise digital zugeschaltet*)
- [REDACTED], Stiftung Digitale Chancen
- [REDACTED], BMI
- [REDACTED], Leibniz-Institut – Hans-Bredow-Institut Hamburg
- [REDACTED], BMFSFJ
- [REDACTED], Universität Hamburg
- [REDACTED], DKHW
- [REDACTED], BMFSFJ
- [REDACTED], BMI
- [REDACTED], Stiftung Digitale Chancen
- [REDACTED], jugendschutz.net (*digital zugeschaltet*)
- [REDACTED], BMFSFJ
- [REDACTED], Gesellschaft für Freiheitsrechte e.V. (*zeitweise*)
- [REDACTED], D64
- [REDACTED], Fraunhofer SIT

6 **Anlagen**

Fotos der Plakatmitschriften 1 bis 3