

# Datensparsame Altersverifikation

York Yannikos, Martin Steinebach

## Einleitung

Das Thema der Altersverifikation im digitalen Raum gewinnt zunehmend an Bedeutung, insbesondere im Kontext des Jugendschutzes. In vielen digitalen Bereichen, beispielsweise Online-Glücksspiel oder Videostreaming, muss die Alterszugehörigkeit von Personen, die diese Bereiche nutzen wollen, zuverlässig verifiziert werden, ohne dass dabei unnötig persönliche Daten preisgegeben werden. Hierbei ist zu beachten, dass die Feststellung einer Alterszugehörigkeit über die einfache Prüfung, ob eine Person beispielsweise volljährig ist oder nicht, hinausgeht. So könnte es etwa für den Zutritt einer Chatgruppe nötig sein nachzuweisen, dass teilnehmende Personen ausschließlich zwischen sechs und 12 Jahren alt sind, wenn eben diese Chatgruppe nur für genau diese Altersgruppe gedacht ist und somit, zum Beispiel zum Schutz gegen Cybergrooming, ältere Personen keinen Zugang haben sollen.

Nachfolgend beschreiben wir eine Methode mittels derer eine Person bestätigen beziehungsweise *verifizieren* lassen kann, dass sie einer gewissen Altersgruppe angehört. Wir betrachten ausdrücklich keine Methode, um das Alter einer Person *festzustellen*, von denen bereits zahlreiche existieren – zum Beispiel mithilfe eines Personalausweises oder per Schätzung durch eine KI-basierte Auswertung eines mit der Smartphone-Kamera übertragenen Videos.

## Hintergrund

Die Altersverifikation im Internet ist eine zentrale Maßnahme zum Schutz Minderjähriger vor ungeeigneten oder potenziell gefährlichen Inhalten. Die rechtliche Grundlage dazu bilden in Deutschland das Jugendschutzgesetz (JuSchG) sowie der

Jugendmedienschutz-Staatsvertrag (JMStV).

Eine wirksame Altersverifikation muss mehreren Anforderungen genügen: Sie muss zuverlässig verhindern, dass nutzende Personen auf nicht altersgerechte Inhalte zugreifen, ohne dabei die informationelle Selbstbestimmung übermäßig einzuschränken. Datenschutzrechtliche Vorgaben, insbesondere die Prinzipien der Datensparsamkeit und Zweckbindung gemäß der Datenschutz-Grundverordnung (DSGVO), müssen beachtet werden. Zudem sollte das Verfahren für eine breite Akzeptanz entsprechend nutzerfreundlich gestaltet sein und Interoperabilität, also die Fähigkeit, dass unterschiedliche Systeme möglichst nahtlos zusammenarbeiten können, mit bestehenden technischen Standards bieten.

Bei der Nutzung von Inhalten im Internet ist neben der Sicherstellung eines Mindestalters auch die Begrenzung eines Höchstalters in bestimmten Bereichen von Bedeutung – insbesondere im Kontext des Schutzes vor Kindesmissbrauch und Cybergrooming. So ist es in sozialen Netzwerken oder auf ähnlichen Plattformen, die sich speziell an Kinder und Jugendliche richten, essenziell, dort sicherzustellen, dass Erwachsene keinen unberechtigten Zugang erhalten. Betreibende solcher Plattformen tragen hierbei die Verantwortung, entsprechende Schutzmechanismen zu etablieren. Hierfür sind neben Altersverifikationen auch KI-gestützte Methoden zur Erkennung von Cybergrooming<sup>1</sup> und für das Profiling hinsichtlich des Alters<sup>2</sup> bekannt.

## Beteiligte

Für eine datensparsame Altersverifikation sind eine Reihe von Beteiligten zu definieren, die jeweils eigene klar definierte Rollen einnehmen:

Die *nutzende* Person möchte auf Inhalte oder Dienste im Internet zugreifen. Diese werden von einem *Dienstanbieter* zur Verfügung gestellt, beispielsweise in Form einer Webseite, eines Streaming-Dienstes oder einer App. Die *verifizierende Instanz* kann die Alterszugehörigkeit der nutzenden Person bestätigen beziehungsweise verifizieren, zum Beispiel aufgrund eines bestehenden Geschäftsverhältnisses, das die Kenntnis des Alters erfordert, oder aufgrund einer ihr vorliegenden behördlichen Auskunft. Um sicherzustellen, dass nur diejenigen Instanzen die Alterszugehörigkeit von Personen bestätigen können, die bestimmten Sicherheitsanforderungen genügen, ist eine *Vertrauensstelle* notwendig. Diese prüft die Vorgehensweise von verifizierenden Instanzen und stellt darauf basierend Zertifikate für diese aus, mit denen sie sich gegenüber Dienstanbietern als berechtigt für eine Altersverifizierung ausweisen können – beispielsweise über eine digitale Signatur.

Um Datensparsamkeit umzusetzen, muss betrachtet werden, wer welche Informationen benötigt. Der nutzenden Person, deren Daten zu schützen sind, sind notwendigerweise sowohl Dienstanbieter als auch verifizierende Instanz bekannt. Der Dienstanbieter benötigt hingegen lediglich eine gültige Bestätigung, dass die nutzende Person einer gewissen Altersgruppe angehört, ansonsten jedoch keine weiteren Informationen. Die verifizierende Instanz weist sich durch die Nutzung eines Zertifikats als vertrauenswürdig aus, das von der Vertrauensstelle ausgestellt wurde. Sie selbst muss dabei nur die Anfrage des Dienstanbieters nach der Alterszugehörigkeit der Person kennen, nicht aber den Dienstanbieter selbst. Weiterhin muss sie die Person und deren Alter kennen, da sie ansonsten keine Bestätigungen bei Altersanfragen zur Person ausstellen könnte. Der Vertrauensstelle sind die Inhalte von Altersanfragen, die von Dienstanbietern an Personen gestellt werden, zu keinem Zeitpunkt bekannt. Ebenso ist ihr nicht bekannt, für welche Altersanfragen welche verifizierende Instanzen Altersbestätigungen ausstellen. Die Vertrauensstelle dient lediglich dazu, die grundlegende Vorgehensweise von verifizierenden Instanzen (regelmäßig) zu prüfen und diesen nach erfolgreicher Überprüfung gültige Zertifikate auszustellen.

## Technische Umsetzung

Bei der technischen Umsetzung einer datensparsamen Altersverifikation betrachten wir lediglich die *Überprüfung* beziehungsweise *Verifikation* einer

Alterszugehörigkeit, nicht jedoch die Feststellung des Alters. Entsprechend wird davon ausgegangen, dass die Feststellung des Alters einer Person, die bei einer verifizierenden Instanz im Vorfeld geschehen sein muss, bereits durchgeführt wurde – beispielsweise durch einen persönlichen Termin bei einem Bürgeramt, das als verifizierende Instanz agiert. Die nutzende Person kann dort dann nach der Altersfeststellung ein Konto erstellen und die notwendigen Zugangsdaten erhalten, um Altersverifikationen durchzuführen. Um zu vermeiden, dass technische oder organisatorische Engpässe entstehen, sind mehrere verifizierende Instanzen vorgesehen, aus denen Personen selbst wählen können, zum Beispiel verschiedene Ämter oder andere Institutionen.

Die Umsetzung der Altersverifikation kann als Protokoll betrachtet werden, das eine Reihe kryptografischer Mechanismen verwendet, um ein möglichst hohes Maß an Datensparsamkeit mit akzeptabler Sicherheit zu erreichen. Das Protokoll basiert auf einem Verfahren, das von den französischen Institutionen Le Laboratoire d'Innovation Numérique de la CNIL (LINC), der École polytechnique und dem Pôle d'Expertise de la Régulation Numérique (PEReN) vorgestellt wurde.<sup>3</sup>

Kernaspekt ist ein Challenge-Response-Verfahren, bei dem ein Dienstanbieter eine Anfrage („Challenge“) an die nutzende Person übergibt, die diese geeignet – eben mithilfe der verifizierenden Instanz – beantworten muss („Response“), um Zugang zu altersbeschränkten Inhalten zu bekommen. Hierbei wird zwischen dem Dienstanbieter und der verifizierenden Instanz niemals direkt kommuniziert, sondern jeglicher Datenaustausch wird stets über die nutzende Person geleitet. Die Abbildungen 1 und 2 zeigen die einzelnen Schritte des Protokolls:

1. Eine nutzende Person fragt bei einem Dienstanbieter Inhalte an, die altersbeschränkt sind, sodass eine Altersverifikation durchgeführt werden muss.
2. Der Dienstanbieter schickt eine Altersanfrage, die aus der Altersanforderung (zum Beispiel „maximal 16 Jahre alt“) und einer zeitlich begrenzten „Challenge“ (zum Beispiel einer sicher erzeugten Zufallszahl) besteht, an die nutzende Person.
3. Die Person meldet sich mit eigenen Zugangsdaten bei der verifizierenden Instanz an, bei der sie zuvor ein Konto eingerichtet hat und schickt an diese die Altersanfrage.
4. Die verifizierende Instanz prüft, ob die Zugangs-

daten korrekt sind, und überprüft dann, ob die Person der angefragten Altersgruppe (hier: „maximal 16 Jahre“) zugehört.

5. Falls dies der Fall ist, bestätigt und signiert die verifizierende Instanz die Altersanfrage samt enthaltener Challenge und schickt diese an die Person zurück.
6. Die Person leitet die signierte und bestätigte Altersanfrage an den Diensteanbieter weiter.
7. Der Diensteanbieter prüft, ob die digitale Signatur gültig ist (also von einer berechtigten verifizierenden Instanz erstellt wurde) und außerdem, ob die Challenge eine von ihm erzeugte, noch gültige Challenge ist.
8. Trifft beides zu, so merkt sich der Diensteanbieter für eine gewisse Zeit, dass die nutzende Person die Altersverifikation erfolgreich durchgeführt hat und liefert ihr die angefragten altersbeschränkten Inhalte aus.

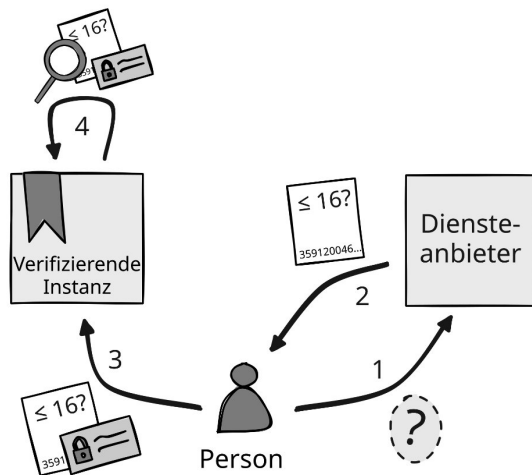


Abbildung 1:  
Schritte 1 bis 4 einer datensparsamen Altersverifikation

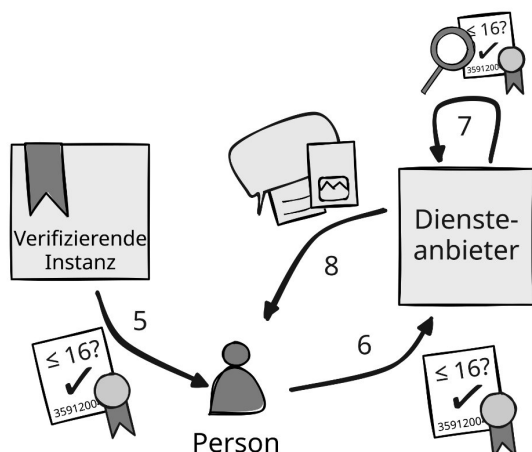


Abbildung 2:  
Schritte 5 bis 8 einer datensparsamen Altersverifikation

Die Vertrauensstelle ist hierbei für die Ausstellung aller Zertifikate für verifizierende Instanzen innerhalb der gesamten Infrastruktur zuständig, mittels derer die digitalen Signaturen ausgestellt werden. Sie kann auch ausgestellte Zertifikate widerrufen, wenn einzelne Instanzen beispielsweise fehlerhafte oder unberechtigte Altersbestätigungen ausstellen.

Bei einem so vorgestellten Verfahren zur Altersverifikation erfährt der Diensteanbieter nicht die Identität der nutzenden Person. Ebenso muss die Person kein Konto beim Diensteanbieter erstellen und auch keine personenbezogenen Daten hinterlegen: Sobald sie altersbeschränkte Daten abrufen möchte, kann sie auf diese für eine gewisse Zeit zugreifen, sobald sie eine Altersverifikation erfolgreich durchgeführt hat. Ist das Zeitfenster des Diensteanbieters für den Zugriff abgelaufen, kann die nutzende Person die Altersverifikation wiederholen. Eine erneute Authentifizierung bei der verifizierenden Instanz ist dabei nicht ständig notwendig, sondern kann beispielsweise auf einmal pro Tag beschränkt werden, sodass die nutzende Person eine Altersverifikation auch automatisch im Hintergrund durchführen und bei sich lokal protokollieren lassen kann, wenn sie das möchte.

## Sicherheit

Aktuell existieren verschiedene Ansätze für eine Altersverifikation im Internet. Allen gemeinsam liegt ein wie oben beschriebenes „Challenge-Response-Verfahren“ zugrunde. Unterschiede bestehen insbesondere darin, wie stark der jeweilige Fokus auf Datenschutz, Sicherheit oder Unabhängigkeit von erforderlichen Geräten (beispielsweise einem Smartphone) gelegt wird. Beim hier vorgestellten Verfahren steht vor allen die Datensparsamkeit, eine einfache Integration in bestehende Infrastruktur sowie möglichst geringe technische Anforderungen an die nutzende Person im Vordergrund. Jedoch ist das Verfahren flexibel gestaltet und kann problemlos an weitere oder andere Anforderungen angepasst werden, zum Beispiel an eine weitere Erhöhung des Datenschutzes durch den Einsatz von speziellen Signaturverfahren mit stärkerem Fokus auf Anonymität, so wie es beispielsweise das Protokollverfahren der französischen Institutionen beschreibt. Ebenso ist eine Erhöhung der Sicherheit möglich, um die ungewollte Weitergabe von signierten Altersanfragen zu erschweren, indem zum Beispiel auf Seite der nutzenden Person zusätzliche kryptografische

Zwischenschritte eingeführt werden.

Wichtig ist zu betonen, dass wir eine datenspar-same Altersverifikation ausdrücklich als Erweiterung bereits existierender Verfahren betrachten, die optional und nicht verpflichtend eingesetzt werden soll. Funktionierende Alternativen stehen mit unterschiedlichen technischen Anforderungen bereits zur Verfügung wie zum Beispiel der Personalausweis mit aktivierter Online-Ausweisfunktion für Personen ab 16 Jahren.

## Literatur

- 1 Shah, A. & Varshney, S. & Mehrotra, M. (2024). Threats on online social network platforms: classification, detection, and prevention techniques. *Multimedia Tools and Applications*. 7 (2024), 1-33.
- 2 HaCohen-Kerner, Y. (2022). Survey on profiling age and gender of text authors. *Expert Systems with Applications*, 199 (117140).
- 3 Gorin, J. & Biéri, M. & Brocas, C. (2022). Demonstration of a privacy preserving age verification process. <https://linc.cnil.fr/demonstration-privacy-preserving-age-verification-process>

## ***Zu den Personen***

**York Yannikos** ist wissenschaftlicher Mitarbeiter und stellvertretender Leiter der Abteilung Media Security and IT Forensics beim Fraunhofer SIT in Darmstadt. Sein Forschungsfokus liegt auf IT-Forensik, OSINT und Privacy by Design.

**Martin Steinebach** leitet die Abteilung Media Security and IT Forensics am Fraunhofer SIT und ist Honorarprofessor an der Technischen Universität Darmstadt. Er koordiniert die Forschungsbereiche REVISE und SenPAI bei ATHENE.