Sachbericht zum Verwendungsnachweis

Teil I Kurzbericht (max. 2 Seiten)

[Stand: 30.03.2023]

Vorhabenbezeichnung:	Schneller elektronischer Identitätsnachweis (SeIn)
Förderkennzeichen:	**16KIS1238**
Laufzeit des Vorhabens:	Bis 30.09.2022 (nach kostenneutraler Verlängerung)
Berichtszeitraum:	Bis einschließlich 30.09.2022

1. Ursprüngliche Aufgabenstellung und Ziel des Vorhabens

Der digitale Binnenmarkt hat das Potenzial, jährlich Wachstumsimpulse in zweistelliger Milliardenhöhe zu generieren und hunderttausende neue Arbeitsplätze in Europa zu schaffen.1 Voraussetzung dafür sind sichere und vertrauenswürdige elektronische Geschäftsprozesse zwischen Unternehmen, Behörden und Bürgern im gesamten EU-Raum. Ausgangspunkt für nahezu alle Geschäftsprozesse im digitalen Binnenmarkt sind sichere und vertrauenswürdige Identitäten, die EU-weit genutzt werden können. Alle Online-Dienste für natürliche und juristische Personen erfordern daher eine schnelle, eindeutige und rechtssichere Identifizierung der Nutzer und Kunden.

Das Problem: Gängige Identifizierungsverfahren mit ausreichendem Vertrauens- und Sicherheitsniveau sind Post-Ident, Video-Ident sowie ID-Karte mit PIN und der neue Personalausweis. Bei all diesen Verfahren gibt es große Einschränkungen entweder durch den Faktor Mensch, hohe Kosten, hohe Abbruchquoten oder durch die benötigte Hardware, die die Benutzerfreundlichkeit und Skalierbarkeit im Alltag stark behindern und einschränken.

Die neue Lösung: Das vorliegende Gründungsprojekt „Schneller elektronischer Identitätsnachweis auf Vertrauensniveau substantiell“ (kurz: SEIN) hat zum Ziel, die Identifizierung von natürlichen und juristischen Personen im digitalen EU-Binnenmarkt zu revolutionieren. Dazu sollen sichere abgeleitete Identitäten unter den rechtlichen Rahmenbedingungen der neuen Zahlungsdiensterichtlinie PSD2 (Konto-Ident) in Kombination mit einer KI-basierten Video-identifikation (Video-Ident) zur Altersverifikation eingesetzt werden.

2. Ablauf des Vorhabens

Wir haben wie geplant eine Komplettlösung (Demonstrator) für eine KI-basierte Videoidentifikation zur Altersverifikation in Echtzeit mit Post-Quantum-Schutz der biometrischen Daten gemäß ISO/IEC IS 24745 und den Kriterien der KJM realisiert.
Damit wurde das Förderziel von StartUpSecure Phase 1 erreicht.

Mit diesem Demonstrator wollten wir in StartUpSecure Phase 2 eine GmbH gründen und in die wirtschaftliche Verwertung gehen. Leider konnte aufgrund der Haushaltssperre des BMBF keine Anschlussfinanzierung für Phase 2 realisiert werden.
Daraufhin hat sich das gesamte Gründer:innen-Team aufgelöst.

3. Die wesentlichen Ergebnisse

Wir haben einen Demonstrator für KI-basierte Video-Identifizierung zur Altersverifikation in Echtzeit mit Post-Quantum-Schutz der biometrischen Daten gemäß ISO/IEC IS 24745 und den Kriterien der KJM realisiert.
Die Kommission für Jugendmedienschutz (KJM) hat das KI-basierte Altersverifikationssystem (videobasiertes Auto-Ident-Verfahren) „Digital-Ident“ des Forschungsprojektes SEIN als Altersverifikationssystem (AVS) geprüft und als AVS-Gesamtlösung in ihre **Positivliste** aufgenommen. [KJM-geprüfte Gesamtlösung zur Altersverifikation: PM 11.11.21]
Entwicklungsbeeinträchtigende und jugendgefährdende Online-Angebote sind heute weit verbreitet. Unser KI-basiertes Auto-Ident-AVS mit post-quantensicherer homomorpher Verschlüsselung der biometrischen Daten und voller Konformität zu ISO/IEC IS 24745 schützt unsere Kinder davor.
Unsere AVS-Gesamtlösung „Digital-Ident“ zur Altersverifikation nach den Kriterien der Kommission für Jugendmedienschutz (KJM) besteht aus einer KI-basierten Video-Erstidentifikation und einer anschließenden Video-Authentifizierung inklusive einer vollständigen homomorphen Verschlüsselung (FHE) zum Langzeitschutz der biometrischen Daten.

Teil-1: KI-basierte Erstidentifizierung (Registrierung beim Online-Anbieter)
KI-basierte Videoidentifikation (auch: Auto-Ident) zur Altersverifikation in Echtzeit mit Ausweisprüfung auf Echtheit und Unversehrtheit, Lebenderkennung und biometrischem Abgleich zwischen biometrischem Ausweisbild und aktuellem Selfie-Video.
Der positiv identifizierte, volljährige Nutzer wird anschließend selbstbestimmt (auf eigenen Wunsch) in einen geschlossenen und geschützten Nutzerkreis aufgenommen. Das biometrische Passbild und das aktuelle Selfie-Foto werden mittels homomorpher Verschlüsselung post-quantensicher in einer geschützten Datenbank hinterlegt.

Teil-2: KI-basierte Authentifizierung (registrierter Nutzer kommt wieder)
KI-basierte Video-Authentifizierung zur Altersverifikation mit Lebenderkennung und biometrischem Abgleich zwischen dem aktuellen Selfie-Foto und den hinterlegten biometrischen Identifikationsdaten (Passfoto und letztes Selfie-Foto).

Innovation 1: Die Implementierung einer homomorphen Verschlüsselung ermöglicht einen umfassenden Schutz der biometrischen Daten. Für den ersten Demonstrator (V0.2) wurde das Cheon-Kim-Kim-Song (CKKS) Verfahren verwendet, da CKKS homomorphe Operationen auf Fließkomma-Templates unterstützt. Das CKKS-Verfahren ist vollständig homomorph (FHE). Jede AVS-Überprüfung erfordert eine Verschlüsselung und einen Vergleich.

Innovation 2: Der biometrische Abgleich zwischen dem neuen, aktuellen Selfie-Foto beim erneuten Besuch des Nutzers beim Online-Anbieter und den bei der Registrierung gespeicherten biometrischen Identifikationsdaten (Passfoto und Selfie-Foto) erfolgt vollständig im verschlüsselten Raum. Die biometrischen Identifikationsdaten bleiben dauerhaft verschlüsselt. Alle notwendigen Rechenoperationen werden im verschlüsselten Raum durchgeführt.

Innovation 3: Homomorphe Verschlüsselung (HE) kann von Quantencomputern nicht gebrochen werden und wird daher als Post-Quanten-sichere Verschlüsselung bezeichnet. Das Post-Quanten-sichere Design garantiert langfristige Datensicherheit.

Sachbericht zum Verwendungsnachweis

Teil II [Stand: 30.03.2023]

Vorhabenbezeichnung:	Schneller elektronischer Identitätsnachweis (SeIn)
Förderkennzeichen:	16KIS1238
Laufzeit des Vorhabens:	Bis 30.09.2022 (nach kostenneutraler Verlängerung)
Berichtszeitraum:	Bis einschließlich 30.09.2022

KI-basierte Altersverifikation und adaptiver Jugendmedienschutz in Echtzeit mit Post-Quanten-gesichertem Schutz der biometrischen Daten nach ISO/IEC IS 24745

Kurz: **Digital-Ident**

Forschungsprojekt SEIN, gefördert durch StartUpSecure (Phase 1) und dem BMBF

Prof. Dr. Michael Massoth
Hochschule Darmstadt
und Nationales Forschungszentrum für angewandte Cybersicherheit *ATHENE*
Email: michael.massoth@h-da.de

Abstract
Jugendmedienschutz durch **KI-basierte Altersverifikation** (Video-basiertes Auto-Ident-Verfahren) in Echtzeit **mit Post-Quanten-sicherem Schutz der biometrischen Daten** nach ISO/IEC IS 24745.
Ein Anwendungsbeispiel, wie mit Künstlicher Intelligenz (KI) und Post-Quanten-Kryptografie, Kinder vor entwicklungs- und jugendgefährdenden Online-Angeboten aus dem Internet geschützt werden können.

Ursprüngliche Aufgabenstellung in StartUpSecure Phase 1

Die Demonstrator-Entwicklung stellt den wesentlichen Bestandteil der Tätigkeiten im Rahmen der StartUpSecure Phase 1 dar. Zu Beginn stehen Tätigkeiten im Vordergrund, die der Entwicklung eines marktfähigen Demonstrators mit minimalen Anforderungen und für den Einsatz in Pilotprojekten dienen.

1a Stand der Forschung/Technik: Altersverifikationssysteme zum Jugendschutz

Altersverifikationssystem (AVS): Ein AVS ist eine Zugangshürde für geschlossene Benutzergruppen im Internet, zu der nur Erwachsene Zugang haben dürfen. AVS müssen nach den Eckwerten und Kriterien der Kommission für Jugendmedienschutz (KJM) die Volljährigkeit des Internetnutzers verlässlich überprüfen: Erstens durch eine Volljährigkeitsprüfung, die über persönlichen Kontakt erfolgen muss, zweitens durch eine Authentifizierung beim einzelnen Nutzungsvorgang.
Es gibt aktuell 11 von der KJM positiv bewertete Gesamtkonzepte, die eine Identifizierung mittels KI-basiertem Auto-Ident-Verfahren anbieten, davon teilweise auch in Kombination mit Video-Identifizierung (mit Call-Center-Agent). [KJM 14.02.22]

Wir präsentieren Ihnen das erste und bislang einzige **KI-basierte Auto-Ident-AVS** mit **Post-Quanten-sicherer homomorpher Verschlüsselung** und vollständigem Schutz der biometrischen Daten nach ISO/IEC IS 24745 (Schutz biometrischer Informationen).

1b Stand der Forschung/Technik beim Schutz biometrischer Daten, Post-Quanten-Kryptografie, Homomorphe Verschlüsselung, ISO/IEC IS 24745-Konformität

Unter Post-Quanten-Kryptografie versteht man kryptografische Verfahren, von denen angenommen wird, dass sie auch mit Hilfe eines Quantencomputers nicht zu brechen sind. Im Gegensatz zur Quantenkryptografie können diese Verfahren schon heute auf klassischer Hardware implementiert werden. [BSI]
Homomorphe Kryptografie ist ein aktuelles Forschungsgebiet der Post-Quanten-Kryptografie. Die Homomorphe Verschlüsselung (HE) stellt den nächsten Evolutionsschritt der Kryptografie dar. [EU Gaia-X]
Verschlüsselung wandelt lesbaren Klartext mittels mathematischer Funktionen in unleserlichen Ciphertext um und nur autorisierte Nutzer*innen, mit passendem privatem Geheimschlüssel, können die Information wieder entschlüsseln und lesen. Bisherige Verschlüsselungsverfahren haben aber einen zentralen Nachteil: Daten sind entweder im Klartext lesbar oder verschlüsselt. Deshalb wurden Daten nur zur Speicherung und zur Datenübertragung verschlüsselt. Verarbeitet werden konnten sie aber bisher nur im Klartext.
Bei der **homomorphen Verschlüsselung (HE)** geht es um das Rechnen mit verschlüsselten Daten, so dass Daten und Datenbanken nun erstmals durchgängig verschlüsselt bleiben und trotzdem genutzt werden können.
Homomorphe Verschlüsselung (HE) ist also ein kryptografisches Verfahren, das homomorphe Operationen auf verschlüsselten Daten ohne deren Entschlüsselung ermöglicht. Für mehr Datenschutz und digitales Vertrauen.

Das Problem und seine Lösung: Entwicklungs- und jugendgefährdende Online-Angebote sind heutzutage weit verbreitet. Unser KI-basiertes Auto-Ident-AVS mit Post-Quanten-sicherer homomorpher Verschlüsselung der biometrischen Daten und vollständiger Konformität zu ISO/IEC IS 24745 schützt unsere Kinder davor.

2 Forschungsergebnisse und Innovationen

Unsere AVS-Gesamtlösung „**Digital-Ident**" zur Altersverifikation nach Kriterien der Kommission für Jugendmedienschutz (KJM), besteht aus einer KI-basierten Erst-Video-Identifizierung und anschließenden Video-Authentifizierung, inklusive einer vollständigen homomorphen Verschlüsselung (FHE) zum langfristigen Schutz der biometrischen Daten.

Teil-1: KI-basierte Erst-Identifizierung (Registrierung beim Online-Anbieter)
KI-basierte Video-Identifizierung (auch: Auto-Ident) zur Altersverifikation in Echtzeit mit Ausweisprüfung auf Echtheit und Unversehrtheit, Lebenderkennung und biometrischem Abgleich zwischen biometrischem Ausweisfoto und dem aktuellen Selfie-Video.
Der volljährige, positiv identifizierte User wird anschließend selbstbestimmt (auf eigenen Wunsch) in einen geschlossenen und geschützten Benutzerkreis aufgenommen. Das biometrische Ausweisfoto und das aktuelle Selfie-Foto werden durch eine homomorphe Verschlüsselung Post-Quanten-sicher in einer geschützten Datenbank hinterlegt.

Teil-2: KI-basierte Authentifizierung (Registrierter User kommt erneut)
KI-basierte Video-Authentifizierung zur Altersverifikation mit Lebenderkennung und biometrischem Abgleich zwischen dem aktuellen Selfie-Foto und den hinterlegten biometrischen Identifizierungsdaten (Ausweisfoto und letzte Selfie-Foto).

Vorteile: Keine erneute Ausweisprüfung mehr notwendig, dadurch rund 50% schnellere Authentifizierung und signifikant höhere Konversionsrate im Vergleich zu einer erneuten Video-Identifizierung mit Ausweisprüfung.

Alle innovativen Features unseres Demonstrators/Prototyps auf einen Blick:
- Spontane WebRTC-Video-Sitzung ohne Installation einer App und ohne Wartezeit
- KJM-geprüfte Gesamtlösung zur Altersverifikation (KJM Positivliste: PM 11.11.21)
- KI-basierte Ausweis-Extraktion mit adaptiver Echtheits- und Unversehrtheitsprüfung der Sicherheitsmerkmale: Holografisches Portrait, 3D-Bundesadler, Personalausweislogo, sowie der kinematischen Bewegungsstrukturen
- KI-basierte Texterkennung (engl. Optical Character Recognition, kurz: OCR), verschiedene Identitätsattribute (wie z.B. Name, Geburtsdatum, Adresse, etc.), inklusive der maschinenlesbaren Zone, werden ausgelesen und auf Echtheit geprüft
- Konsistenzprüfung der Daten auf Vorderseite und Rückseite des Ausweisdokuments
- Konsistenzprüfung von Geburtsdatum mit Prüfziffer, Gültigkeitsdatum mit Prüfziffer, Ländercode, und Gesamtprüfziffer (MRZ-Prüfziffern)
- KI-basierte Lebenderkennung wahlweise durch 4-5 Gesten-Challenges, und/oder Text-Vorlese-Challenges
- KI-basierte Altersschätzung als zusätzliche Plausibilitätsprüfung
- 2-Faktor-Authentifizierung für den bereits registrierten User wahlweise mit Eingabe der Ausweis-Seriennummer und/oder 6-stelliger SMS-TAN (One-Time-Password)
- Alle erhobenen Daten werden mithilfe symmetrischer und asymmetrischer Kryptografie gesichert. Homomorphe Verschlüsselung ermöglicht einen umfassenden Schutz der biometrischen Daten und volle ISO/IEC IS 24745-Konformität.

- Das AVS-System kommuniziert ausschließlich über TLS gesicherte Verbindungen
- Sehr gute User Experience durch User-centered Design und Security
- Vollständig DSGVO-konforme Lösung mit Serverbetrieb in Deutschland
- Schon kompatibel mit 98% aller Web-Browser in Deutschland

Innovation 1: Die Implementation einer **homomorphen Verschlüsselung** ermöglicht einen umfassenden Schutz der biometrischen Daten. Für den ersten Prototypen wurde dazu das Cheon-Kim-Kim-Song (CKKS)-Verfahren benutzt, weil CKKS homomorphe Operationen auf Gleitkomma-Vorlagen unterstützt. Das CKKS-Verfahren ist vollständig homomorph (FHE). Jede AVS-Überprüfung erfordert eine Verschlüsselung und einen Vergleich.

Innovation 2: Der **biometrische Abgleich** zwischen dem neuen, aktuellen Selfie-Foto beim erneuten Besuch des Users beim Online-Anbieter und den bei der Registrierung gespeicherten biometrischen Identifizierungsdaten (Ausweisfoto und Selfie-Foto) wird komplett **im verschlüsselten Raum** durchgeführt. Die biometrischen Identifizierungsdaten bleiben **dauerhaft verschlüsselt** und werden niemals unverschlüsselt benutzt. Alle notwendigen Rechenoperationen werden im verschlüsselten Raum vorgenommen.

Innovation 3: Homomorphe Verschlüsselung (HE) kann durch Quanten-Computer nicht gebrochen werden und gilt deshalb als Post-Quanten-sichere Verschlüsselung. Durch das Post-Quanten-sichere Design wird eine **langfristige Datensicherheit** gewährleistet.

Innovation 4: Unser Prototyp zeigt, dass Altersverifikation mit Gesichtserkennung im verschlüsselten Bereich für biometrische Gesichtsvorlagen **in Echtzeit** möglich ist.
Unsere Ergebnisse zeigen außerdem die **Praxistauglichkeit** des Schutzes biometrischer Gesichtsvorlagen für die Alters- und Gesichtsverifikation (allgemein für AVS-Systeme) **auf handelsüblicher Hardware**.

Innovation-5: Alle drei Datenschutzanforderungen der **ISO/IEC 24745** nach Irreversibilität, Unverknüpfbarkeit und Vertraulichkeit in einer vertrauensfreien Umgebung, werden von unserem FHE-Verfahren voll erfüllt. Unser Prototyp hat damit volle ISO/IEC IS 24745-Konformität.

Die Datenschutzanforderungen der ISO/IEC 24745 sind:
(i) Irreversibilität: Für eine bestimmte vordefinierte Verwendung (z. B. AVS mit Gesichtserkennung) müssen die biometrischen Rohdaten in eine irreversible Repräsentation umgewandelt werden, die genau der Aufgabe der vordefinierten Verwendung entspricht.
(ii) Unverknüpfbarkeit: Es darf keine Beziehung zwischen den gespeicherten biometrischen Templates geben, weder über Anwendungen noch über Datenbanken hinweg.
(iii) Vertraulichkeit: Das biometrische Template muss sicher aufbewahrt werden und darf nicht für Unbefugte zugänglich sein, die versuchen, sich unerlaubten Zugang zu verschaffen.

Durch die vollständige Erfüllung der oben genannten Anforderungen wird die Privatsphäre des Benutzers, sowohl während des Vergleichs (der 2-Faktor-Authentifizierung), als auch bei durchgesickerten oder gar gestohlenen biometrischen Vorlagen, langfristig geschützt.

3 Nutzen für Wirtschaft und Gesellschaft

Nutzen für Kinder und Jugendliche: Kinder sind im Durchschnitt elf Jahre alt, wenn sie das erste Mal Pornografie sehen [TKK, 26.08.21]. Wir schützen Kinder vor entwicklungs- und jugendgefährdenden Online-Angeboten aus dem Internet.

Nutzen für Unternehmen: Online-Anbieter bestimmter unzulässiger, verbotener und jugendgefährdender Internet-Angebote können sich gesetzeskonform verhalten, indem sie ihren Angeboten unser **KJM-geprüftes AVS** für geschlossene Benutzergruppen vorschalten. Dabei wird die Barriere für volljährige Kunden so gering als möglich gehalten, ohne die Sicherheit für Kinder zu beschneiden

Gesamtgesellschaftlicher Aspekt (Nutzen für unsere Gesellschaft):
Die junge Generation ist aufgrund der Corona-Pandemie mit Lockdown, Homeschooling und Kontaktsperren mehr denn je ins Internet gezogen. Das bedeutet für den Kinder- und Jugendmedienschutz in Deutschland mehr Verantwortung als je zuvor.
Pornografie darf in Deutschland nach § 184 StGB grundsätzlich nur Personen über 18 Jahren zugänglich gemacht werden. Dadurch sollen Minderjährige vor dem unerlaubten Zugänglichmachen von pornografischen Bildern, Darstellungen oder Filmen geschützt werden. Die Wirklichkeit in Deutschland sieht jedoch anders aus.
Bei wissenschaftlichen Online-Befragungen [Vogelsang 2017, SPRINGER] gaben 86% der Jungen und 39% der Mädchen aus der Altersgruppe 14-17 an, schon gezielt Online-Pornografie konsumiert zu haben. Davon konsumieren 31,7% der Jungen und 6,9% der Mädchen mehrmals in der Woche Pornografie. Besonders erschreckend: 9,2% der Jungen und 1,4% der Mädchen gaben an, täglich Online-Pornografie zu konsumieren (Pornosucht). Die Hälfte aller Eltern macht sich Sorgen, dass Online-Pornografie ihren Kindern eine unrealistische Sicht auf Sex gibt. Mehr als die Hälfte der Mütter haben Angst, dass die Inhalte ihren Kindern ein schlechtes Frauenbild vermittelt.
Deutsche Jugendschützer können von Internetanbietern die Sperrung der Online-Pornoportale verlangen, wenn diese das Alter ihrer Nutzer nicht verifizieren.
Lange Zeit galt Pornosucht als ein Randphänomen, heute ist sie eine ernstzunehmende Krankheit: Schätzungen zufolge leiden etwa eine halbe Million Menschen in Deutschland darunter. Tendenz steigend. [TKK, 26.08.21]

Altersverifikation bei Online-Sportwetten und Glücksspielen:
Wissenschaftliche Studien zeigen, dass Jugendliche breiten Zugang zu Glücksspielen haben. Etwa 10% der 14- bis 17-Jährigen nehmen regelmäßig an Glücksspielen teil.
Jugendliche haben einen großen Hang zur Spielsucht. Die erhöhte Risikobereitschaft, das fehlende Verantwortungsbewusstsein und die Suche nach Spaß und Aufregung sind klare Indizien dafür, dass der Jugendschutz auch bei Online-Sportwetten und Glücksspielen zwingend erforderlich ist.
Das Jugendschutzgesetz verbietet es Jugendlichen unter 18 Jahren, an Sportwetten und Glücksspielen teilzunehmen. Ein verlässlicher Alters- und Identitätsnachweis wird von den Online-Anbietern aber meist erst vor der ersten Gewinn-Auszahlung eingefordert.

4 Marktchancen

Starker, großer Wachstumsmarkt: Der europäische Markt für Identitätsverifizierung wird voraussichtlich von 1,46 Mrd. USD im Jahr 2018 auf 4,40 Mrd. USD im Jahr 2027 wachsen. Dies entspricht einer **durchschnittlichen jährlichen Wachstumsrate von 13,3%** von Jahr 2018 bis 2027. [The INSIGHT Partners]
Mit Fokus auf Altersverifikation und Jugendmedienschutz im KJM-regulierten Markt.

Videospiele mit FSK 16 oder älter hatten im Jahr 2020 einen Marktanteil von 30,3%.
Durch den wachsenden **Online-Handel** mit Lebensmittel sind schon jetzt Altersverifikationen für den Erwerb von Tabakwaren und alkoholischen Getränke dringend notwendig.
Im Marktsegment **Online-Sportwetten** wurden 2020 laut STATISTA in Deutschland Umsätze von 7,79 Milliarden Euro gemacht. Online-Befragungen ergaben, dass rund 6% der deutschen Bevölkerung (zwischen 18 und 64 Jahren) Online-Sportwetten abschließen.

Viele weitere Marktsegmente: Neben der Altersverifikation bei FSK18 Angeboten (inklusive Online-Pornografie, Online-Sportwetten und Online-Gaming), Prepaid SIM-Karten oder Versicherungen, besteht im **E-Commerce** und **Online-Handel** auch ein starker Identifizierungswunsch seitens der Online-Anbieter. Denn Versicherungen, Energieversorger, Vergleichsplattformen, Medien-Plattformen, Reisebuchungsplattformen, Online-Shops, Airlines, und weitere Branchen wie z.B. Spendenorganisationen und Loyalty-Programme möchten ihre User ebenfalls sicher identifizieren, um Betrug oder Missbrauch vorzubeugen.

Preismodelle: Die AVS-Gesamtlösung von Digital-Ident baut auf einer flexiblen Preisstruktur auf, welche es einem Online-Anbieter (Geschäftskunden) ermöglicht zwischen den Modellen einer Nutzungsgebühr („Pay-per-transaction"), Mitgliedsgebühr (Monatlicher Abonnement) und einem Sammelverkauf (Verkauf einer vordefinierten Anzahl an Altersverifikationen) zu entscheiden und flexibel zu wechseln.

- Preis für eine Altersverifikation (Erst-Identifizierung): 0,50 €
- Preis für eine 2-Faktor-Authentifizierung (Registrierter User kommt erneut): 0,25 €

Vertrieb: Digital-Ident hat Vertraulichkeitsvereinbarungen mit den beiden erfolgreichsten IT-Ausgründungen der Hochschule Darmstadt: Mit der AUTHADA GmbH, Darmstadt, und der bevelop GmbH, Aschaffenburg. Beide IT-Unternehmen haben Geschäftskunden, die an der schnellen und zuverlässigen Altersverifikation von Digital-Ident sehr interessiert sind. Die interessierten Geschäftskunden kommen aus den fokussierten Marktsegmenten: Jugendmedienschutz bei Pornografie und Sportwetten.

Breakeven innerhalb von 3-6 Monaten: Die Anzahl benötigter Altersverifikationen pro Monat [Transaktionen pro Monat] sind in den Marktsegmenten Jugendmedienschutz so hoch, dass bereits ein einziger Pilotkunde die Chance auf einen Breakeven innerhalb von 3-6 Monaten eröffnet. Beleg: Allein die Pornoseite Pornhub verzeichnete im Jahr 2020 rund **15,6 Millionen tägliche Besuche** aus Deutschland.

5 Wesentliche Ergebnisse und aktueller Stand des Demonstrators

Wir haben einen Demonstrator für KI-basierte Video-Identifizierung zur Altersverifikation in Echtzeit mit Post-Quantum-Schutz der biometrischen Daten gemäß ISO/IEC IS 24745 und den Kriterien der KJM realisiert.

Die Kommission für Jugendmedienschutz (KJM) hat das KI-basierte Altersverifikationssystem (videobasiertes Auto-Ident-Verfahren) „Digital-Ident" des Forschungsprojektes SEIN als Altersverifikationssystem (AVS) geprüft und als AVS-Gesamtlösung in ihre **Positivliste** aufgenommen. [KJM-geprüfte Gesamtlösung zur Altersverifikation: PM 11.11.21]

Entwicklungsbeeinträchtigende und jugendgefährdende Online-Angebote sind heute weit verbreitet. Unser KI-basiertes Auto-Ident-AVS mit post-quantensicherer homomorpher Verschlüsselung der biometrischen Daten und voller Konformität zu ISO/IEC IS 24745 schützt unsere Kinder davor.

Unsere AVS-Gesamtlösung „Digital-Ident" zur Altersverifikation nach den Kriterien der Kommission für Jugendmedienschutz (KJM) besteht aus einer KI-basierten Video-Erstidentifikation und einer anschließenden Video-Authentifizierung inklusive einer vollständigen homomorphen Verschlüsselung (FHE) zum Langzeitschutz der biometrischen Daten.

Teil-1: KI-basierte Erstidentifizierung (Registrierung beim Online-Anbieter)
KI-basierte Videoidentifikation (auch: Auto-Ident) zur Altersverifikation in Echtzeit mit Ausweisprüfung auf Echtheit und Unversehrtheit, Lebenderkennung und biometrischem Abgleich zwischen biometrischem Ausweisbild und aktuellem Selfie-Video.
Der positiv identifizierte, volljährige Nutzer wird anschließend selbstbestimmt (auf eigenen Wunsch) in einen geschlossenen und geschützten Nutzerkreis aufgenommen. Das biometrische Passbild und das aktuelle Selfie-Foto werden mittels homomorpher Verschlüsselung post-quantensicher in einer geschützten Datenbank hinterlegt.

Teil-2: KI-basierte Authentifizierung (registrierter Nutzer kommt wieder)
KI-basierte Video-Authentifizierung zur Altersverifikation mit Lebenderkennung und biometrischem Abgleich zwischen dem aktuellen Selfie-Foto und den hinterlegten biometrischen Identifikationsdaten (Passfoto und letztes Selfie-Foto).

Innovation 1: Die Implementierung einer homomorphen Verschlüsselung ermöglicht einen umfassenden Schutz der biometrischen Daten. Für den ersten Demonstrator (V0.2) wurde das Cheon-Kim-Kim-Song (CKKS) Verfahren verwendet, da CKKS homomorphe Operationen auf Fließkomma-Templates unterstützt. Das CKKS-Verfahren ist vollständig homomorph (FHE). Jede AVS-Überprüfung erfordert eine Verschlüsselung und einen Vergleich.

Innovation 2: Der biometrische Abgleich zwischen dem neuen, aktuellen Selfie-Foto beim erneuten Besuch des Nutzers beim Online-Anbieter und den bei der Registrierung gespeicherten biometrischen Identifikationsdaten (Passfoto und Selfie-Foto) erfolgt vollständig im

verschlüsselten Raum. Die biometrischen Identifikationsdaten bleiben dauerhaft verschlüsselt. Alle notwendigen Rechenoperationen werden im verschlüsselten Raum durchgeführt.

Innovation 3: Homomorphe Verschlüsselung (HE) kann von Quantencomputern nicht gebrochen werden und wird daher als Post-Quanten-sichere Verschlüsselung bezeichnet. Das Post-Quanten-sichere Design garantiert langfristige Datensicherheit.

Prozessablaufdiagramm

Zuerst identifiziert sich der/ die Nutzer:in mittels Ausweises und Selfie-Videos. Die Digital Ident-Lösung nimmt den/die Benutzer:in mithilfe einer eigens entwickelten KI-gestützte Bilderkennung mit seiner Smartphone-Kamera auf. Der Personalausweis wird ebenfalls von dem/der Nutzer:in fotografiert (Vorder- und Rückseite). Dann kann die Digital Ident-Lösung die biometrischen Daten miteinander abgleichen. Nach der Bestätigung durch den/die Nutzer:in ist der erste Schritt von Auto-Ident abgeschlossen.

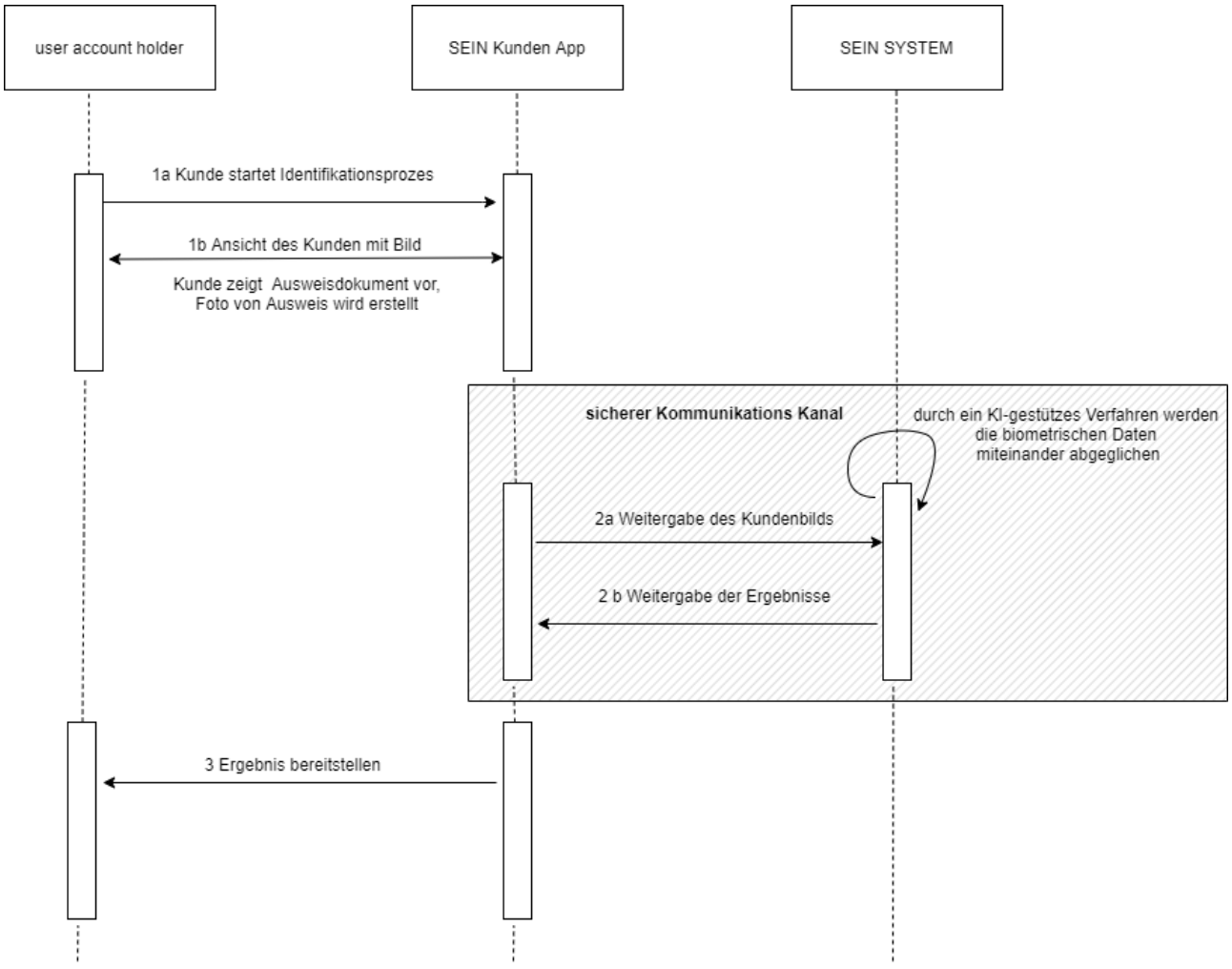

Abbildung 1: Technische Funktionsweise Identifikationsprozess per Video

Innovation 4: Unser Demonstrator zeigt, dass Altersverifikation mit Gesichtserkennung im verschlüsselten Bereich für biometrische Gesichtstemplates in Echtzeit möglich ist.

Unsere Ergebnisse zeigen auch die Praxistauglichkeit des Schutzes von biometrischen Gesichtstemplates für die Alters- und Gesichtsverifikation (allgemein für AVS-Systeme) auf normaler, kommerzieller Hardware.

Innovation 5: Alle drei Datenschutzanforderungen der ISO/IEC 24745 nach Irreversibilität, Unverknüpfbarkeit und Vertraulichkeit in einer vertrauensfreien Umgebung werden von unserem FHE-Verfahren vollständig erfüllt. Unser Demonstrator ist somit vollständig ISO/IEC IS 24745 konform.

Durch die vollständige Erfüllung der oben genannten Anforderungen wird die Privatsphäre des Benutzers langfristig geschützt, sowohl während des Vergleichs (der 2-Faktor-Authentifizierung), als auch im Falle eines Durchsickerns oder gar Diebstahls des biometrischen Templates.

6 Notwendigkeit und Angemessenheit der geleisteten Projektarbeit

Am Ende der StartUpSecure Phase 1 hat das Entwicklungsprojekt „Schneller elektronischer Identitätsnachweis" (kurz: SEIN) außerdem nachfolgende Ziele erreicht:

Thema	**Beschreibung**
Serverinfrastruktur	Einrichtung der Serverumgebung mit Tests und Sicherheitsbewertung gemäß der DSGVO in Rechenzentren in Frankfurt am Main und in Düsseldorf.
Demonstrator	Entwicklung einer Customer Journey mit Auswahl der Identifikationstechnologien und Definition der Identifikationsschritte.
	Konto-Ident: Konzeptentwicklung von UX / UI. Es wurden klickbare „Prototypen" für zwei Use-Cases erstellt, jeweils als embedded-Version (also Pop-up) und redirect-Version (Weiterleitung zur Bank).
	Frontend- und Backend-Entwicklung des Identifizierungs-Snippets, einer Verwaltungsoberfläche (interne Nutzung) und eines Geschäfts-kundenportals (Self-Service Plattform für Onlinedienste-anbieter, die die Digital Ident-Lösung nutzen). Die Entwicklung wurde gefolgt von einer Sicherheitsüberprüfung aller Softwarekomponenten und der Betriebsumgebung an die Nutzerverhältnisse angepasst.
	Erstellung eines Design-Prototyps für die Durchführung von Usability-Tests.
Präzisierung von Use Cases	Marktanalyse und Entwicklung von Use-Cases unter Berücksichtigung aktueller Entwicklungen im Markt. Erstellung von User Personas.
	Durchführung eines UX Software Tests mit internen und externen Tester:innen sowie Studierendengruppen der Hochschule Darmstadt.
Compliance	Beantragung der BaFin Registrierung als Kontoinformationsdienst gemäß §34 Zahlungsdienstaufsichtsgesetz vorbereitet.
	ISO 27001 Zertifizierung nach BSI TR-03147, um in relevanten Branchen (insbesondere E-Government) als Identitätsdienstleister tätig werden zu können, wurde beantragt. Das erste Audit wurde bereits erfolgreich absolviert.

	Einrichtung einer auf Scrum-Systemen basierenden Projektkoordinationsumgebung mit wöchentlichem Status-Reporting.
	Kontinuierliche Dokumentation von Softwarekomponenten einschließlich des Codes der Software-Komponenten und der Serverinfrastrukturen.
Kommunikation und Technologietransfer	Einrichtung der Digital-Ident Domain und einem ersten Designlayout des Projekt-Website-Inhalts.
	Richtlinien für Social Media-Profile und Entwurf eines Content-Plans.

Zusammenfassend lässt sich feststellen:
Alle oben beschriebenen Projektarbeiten waren sowohl notwendig als auch angemessen.

7 In StartUpSecure Phase 2 geplante Projektarbeiten

Ein lauffähiger Demonstrator für PSD2-Konto-Ident war innerhalb der verbleibenden Rest-Laufzeit von StartUpSecure Phase 1 leider nicht möglich, wie uns unsere Anwaltskanzlei ANNERTON glaubhaft versichert hat.
Unsere Anwälte von ANNERTON hatten uns 12/2021 darüber informiert, dass sich die Bearbeitungszeiten der BaFin für die Beantragung der PSD2-KID-Lizenz von früher regulär 3 Monate auf aktuell 8-12 Monate verlängert haben.
Diese signifikante und unvorhersehbare Verlängerung der Bearbeitungszeiten der BaFin auf 8-12 Monate für die Beantragung der PSD2-KID-Lizenz, ist hauptsächlich dem Wirecard Skandal geschuldet. Die Bearbeitungszeiten von 8-12 Monaten gilt ab Vollständigkeit aller Antragsdokumente. Im Dezember 2021 hatten wir mithilfe der Anwaltskanzlei ANNERTON erst rund 1/3 der notwendigen Antragsdokumente in einem einreichungsfähigen Zustand. Außerdem war bis Ende 2021 auch das gesamte Budget für juristische Unterstützung der Antragstellung bei der BaFin von rund 39.000 € aufgebraucht. Deshalb wurde der Konto-Ident-Demonstrator sowie die Registrierung als Kontoinformationsdienstleister bei der BaFin auf die StartUpSecure Phase 2 verschoben.

In StartUpSecure Phase 2 waren nachfolgende Projektarbeiten geplant:

Im zweiten Schritt verifiziert die Digital Ident-Lösung die Kontoinhaberschaft des/der Nutzers:in zu seinem Referenzkonto. Dabei wird zusätzlich eine 2-Faktor-Authentifizierung geprüft, indem der Prozess den Besitz des Smartphones und das Wissen der Konto-Login-Daten voraussetzt. Über das von dem/der Nutzer:in angegebene Konto löst die Digital Ident-Lösung eine Referenzüberweisung aus. Die erfolgreiche Referenzüberweisung verifiziert den/die Nutzer*in als legitimen Kontoinhaber.

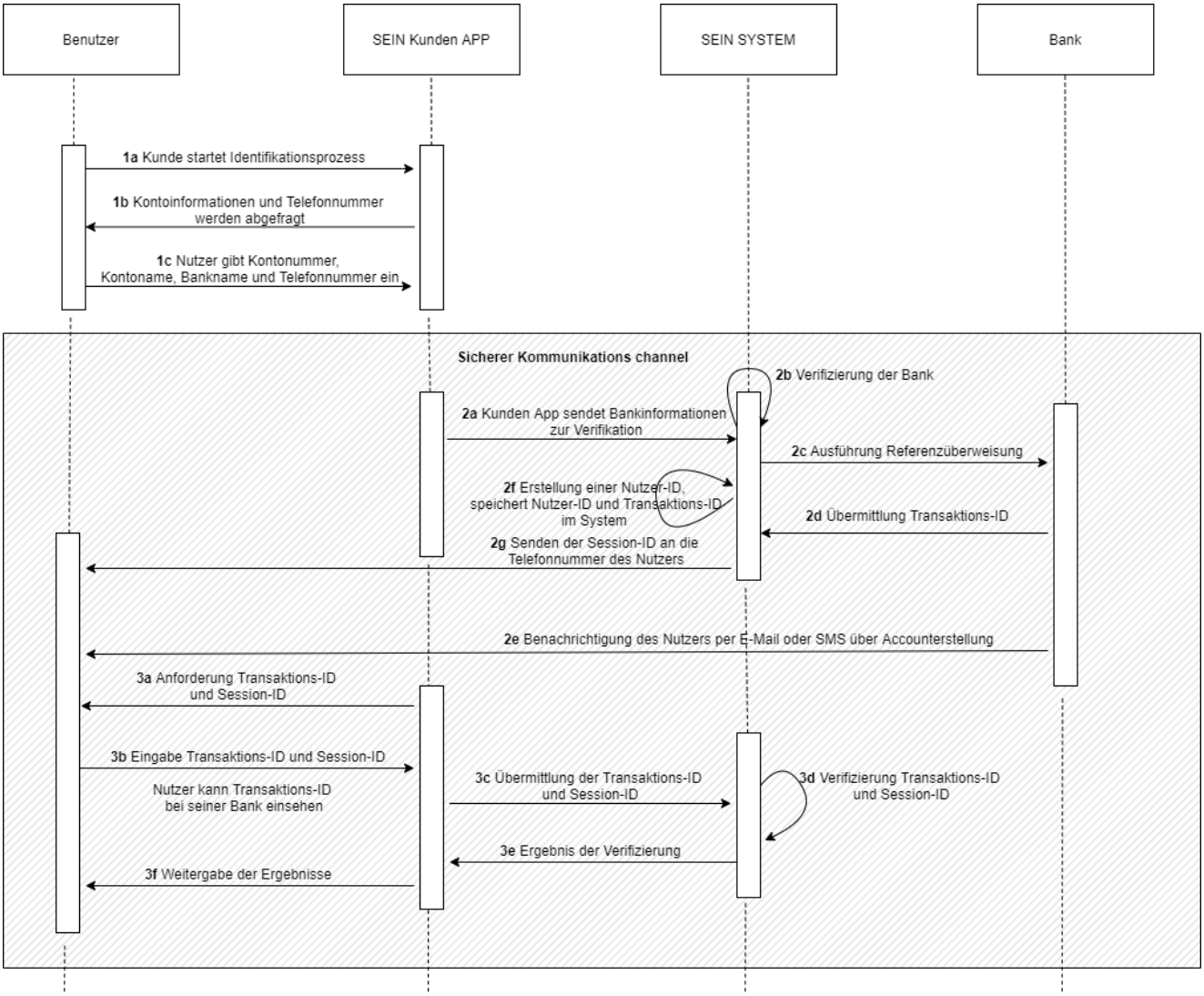

Abbildung 2: Technische Funktionsweise der Kontoverifizierung

Zusätzlich soll die PSD2-Registrierung als Kontoinformationsdienst genutzt werden, um ein Bonitätsbewertungsmodell auf Basis der Kontoinformationen zu entwickeln. Der/Die Nutzer:in, der/die durch den Konto-Login Kontoinformationen freigibt, kann so auf seine/ihre Zahlungsfähigkeit und seine/ihre Zahlungsmoral hin überprüft werden. Gemäß der PSD2-Verordnung von 2005 können die folgenden Daten von Kontoinformationsdiensten eingesehen und analysiert werden: Name des/der Kontoinhabers:in, Kontostand, Tagessalden (historisch 89 Tage), Verwendungszweck, Überziehungslimit und weitere Flags, die Eigenschaften der einzelnen Kontotransaktionen markieren (z.B. Rückbuchungen, Inkassozahlungen). Basierend auf der in Phase I entwickelten Technologie und der erworbenen Lizenz als ISO-zertifizierter KID, wird Digital Ident zwei zusätzliche, für Online-Händler werthaltige Informationen, ermitteln können:

Liquiditätsbestätigung: Mithilfe des Kontostands und dem genehmigten Überziehungslimit kann die Liquidität zum Zeitpunkt der Online-Transaktion ermittelt werden und in real-time an den Online-Händler übermittelt werden. Somit können wir dem Online-Händler nicht nur die Identität des/der Nutzers:in nachweisen, sondern gleichzeitig seine Zahlungsfähigkeit bestätigen.

Bonitätsbestätigung: Darüber hinaus soll auf Basis der gesamten Kontotransaktionsdaten eine Logik entwickelt werden, die eine Echtzeit-Bewertung der Bonität des/der Nutzers:in ermöglicht. Für diese Analyse werden vor allem der aktuelle Kontostand, die Tagessalden der letzten 89 Tage, die Verwendungszwecke und das Überziehungslimit herangezogen. Der kritische Teil, welcher auch vom Wettbewerb aktuell nur schlecht umgesetzt wird, ist die Textanalyse in den Verwendungszwecken. In Kombination mit den Flags zu Rücklastschriften und Inkassozahlungen soll eine Bonitätsbewertung während des Kaufprozesses stattfinden, die genau wie die Liquiditätsbestätigung in Echtzeit an den Online-Händler übermittelt werden soll. Die technische Funktionsweise und die Datenübertragung findet wie bei der in Phase I entwickelten Identitätsprüfung statt (siehe Abbildung 3).

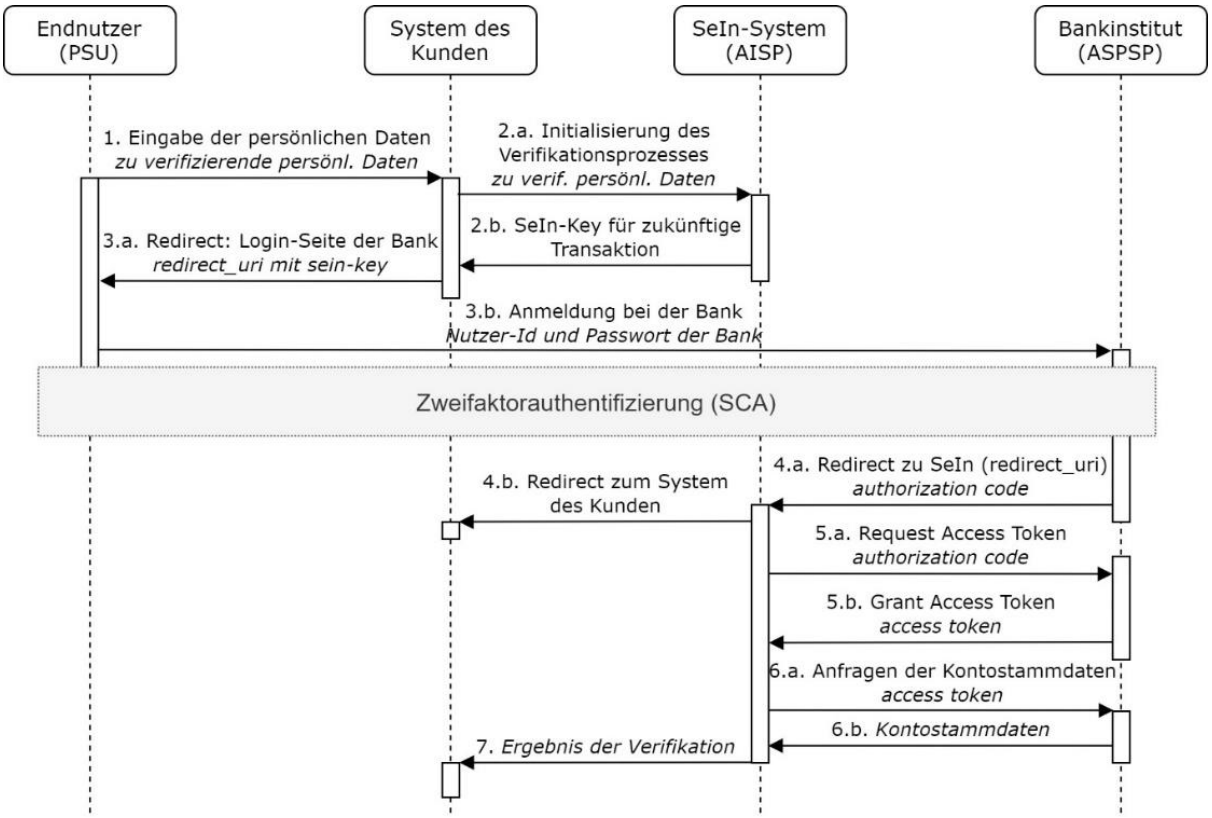

Abbildung 3: Technische Funktionsweise und Datenübertragung

8 Wissenschaftliche und wirtschaftliche Anschlussfähigkeit

Wir waren bereit für StartUpSecure Phase 2 und die Ausgründung als GmbH. Leider war aufgrund der 8-monatigen Haushaltssperre des BMBF nach der Bundestagswahl 2021 keine Anschlussfinanzierung möglich. Als unmittelbare Konsequenz hat sich das gesamte Gründerteam aufgelöst. Alle wissenschaftlichen Mitarbeiter:innen und Gründer:innen haben sich neue, unbefristete Stellen in Industrie und Wirtschaft gesucht.
Aufgrund der kostenneutralen Verlängerung und des geringen Restbudgets waren auch keine Neueinstellungen (seitens unserer HDA-Verwaltung) mehr möglich.