Self-Sovereign Identity und Identitätsprüfung nach dem GwG

Dr. Christian Lange-Hausstein*

Dieser Beitrag stellt dar, wie das Konzept der „Self-Sovereign Identity" von GwG-Verpflichteten zur Identifizierung genutzt werden kann und welche Rolle die zu diesem Zweck in § 13 GwG eingefügte „Experimentierklausel" spielt.

I. Einführung

Digitale Identitäten sind heute oft zentral bei Gatekeepern[1] oder bei Identitätsanbietern angelegt. Wenn die „Logins" dieser Unternehmen in Webseiten und Apps Dritter eingebunden werden, kann das Verhalten der Nutzenden über alle Dienste hinweg verfolgt werden. Nutzenden nimmt das ihre „digitale Souveränität". Die EU-Kommission, die Bundesregierung und Initiativen aller Sektoren setzen dem dezentrale Identitätskonzepte entgegen, die die Identitätsdaten in die Hand der jeweiligen Person legen.

II. Das Self-Sovereign Identity-Konzept

Der Begriff Self-Sovereign-Identity („SSI") beschreibt keine feststehende Infrastruktur aus Hardware und Software. Stattdessen steht SSI, wie auch etwa der Begriff Distributed Ledger Technologie („DLT"), für ein Konzept. Die Grundidee des SSI-Konzepts ist, dass die Person, die ein Identitätsmerkmal betrifft, ausschließlich selbst darüber entscheidet, wem gegenüber sie das Merkmal offenlegt. Die Organisation, die das Identitätsmerkmal ausstellt, erfährt in SSI-Infrastrukturen nicht, dass das Identitätsmerkmal benutzt wird. Verdeutlichen lässt sich das anhand des „analogen" Vorbilds Personalausweis: Wann, wo und wem eine Person den Ausweis zum Beleg ihrer Identität vorlegt, erfahren weder die Personalausweisbehörde noch die Bundesdruckerei, sondern nur die Person selbst und die jeweilige Stelle, vor der sie sich identifiziert. SSI wird deshalb auch als Beitrag zur Datensouveränität des Einzelnen verstanden.[2] In Deutschland treten zwei Initiativen besonders hervor: Seit Ende 2019 arbeiten Organisationen aus Wirtschaft, Forschung und Verwaltung in einem vom Bundesministerium für Wirtschaft und Energie (BMWi) geförderten sog. „Schaufensterprojekt" am Aufbau eines offenen Ökosystems dezentraler digitaler Identitäten.[3] Das Bundeskanzleramt, verschiedene Ministerien und rund 20 Unternehmen aus unterschiedlichen Sektoren begannen Ende 2020 mit der Entwicklung des Projekts „Ökosystem Digitale Identitäten".[4] In der Schweiz hat Ende 2021 der Bundesrat festgelegt, dass die staatliche digitale Identität nach SSI-Grundsätzen ausgestaltet werden soll.[5]

1. SSI-„Rollen" und Infrastruktur

Eine einheitliche Terminologie hat sich zwischen den diversen Initiativen noch nicht herausgebildet. Für die Zwecke dieses Beitrags gilt das folgende Begriffsverständnis. Es orientiert sich wegen ihrer Relevanz für die geldwäscherechtlichen Anwendungsfälle v. a. an den bis dato veröffentlichten Ergebnissen des Projekts „Ökosystem Digitale Identitäten" des Bundeskanzleramts. Abstrakt sieht das SSI-Konzept drei „Rollen" vor. Eine vierte Rolle kommt hinzu, wenn das Konzept praktisch in der Form von Apps anwendbar gemacht wird. Alle Rollen des SSI-Konzepts können von natürlichen Personen oder juristischen Personen des Privatrechts oder des öffentlichen Rechts eingenommen werden.

a) Haltende Person und ihre Identitätsmerkmale

Die zentrale Rolle hat die sog. „haltende Person". Sie wird auch „Inhaber" oder „Holder" genannt. Als haltende Personen kommen insbesondere natürliche Personen in Betracht, die bestimmte Identitätsmerkmale „halten". Diese Identitätsmerkmale werden auch „Attribute" oder „Claims" genannt. Das können zum Beispiel Informationen über die Person selbst sein, wie etwa ihr Name und ihre Anschrift. Identitätsmerkmale können auch sonstige Informationen sein, wie bspw. akademische Abschlüsse, die Führerscheinklasse oder der Einkommenssteuerbescheid[6]. Die genannten Beispiele für Identitätsmerkmale haben gemein, dass sie von vertrauenswürdigen Herausgebern als verschlüsselte, signierte und verifizierte Nachweise ausgestellt wurden (sog. „Verified Credentials"). Daneben besteht die Möglichkeit, dass haltende Personen sich Merkmale selbst ausstellen (sog. „Self-Attested Attributes"). Das kann für die Praxis relevant sein, wenn bspw. im Zusammenhang mit Vertragsschlüssen die E-Mail-Adresse oder die Telefonnummer über die SSI-Infrastruktur übermittelt werden soll.

Schließlich ist nicht zwingend, dass die haltende Person eine natürliche Person ist. In anderen, hier nicht weiter diskutierten Fällen, kann die haltende „Person" auch eine Verwaltungsstelle, eine Maschine oder ein Bauteil sein.[7] Diese Fälle betreffen zum Beispiel die Machine-to-Machine-Kommunikation, in der sich etwa

ein Thermostat gegenüber einem Versorgungsnetz oder ein Auto gegenüber einer E-Ladesäule „identifiziert".[8]

b) Ausstellende Organisation

Ausstellende Organisationen sind die privaten oder öffentlichen Stellen, die einen Nachweis über ein Identitätsmerkmal ausstellen können. Sie werden auch „Herausgeber" oder „Issuer" genannt. Die Ausstellung erfolgt stets erst auf Betreiben der haltenden Person. Als ausstellende Organisation kommen bspw. in Betracht: die Bundesdruckerei (etwa für die Basis-ID), Universitäten (für akademische Abschlüsse), das Kraftfahrzeugbundesamt (für die Führerscheinklasse), das örtliche Finanzamt (für den Einkommenssteuerbescheid), die Bank (für die hier sog. „Bank-ID").

c) Verifizierende Organisation

In der Rolle der verifizierenden Organisation kann jede Einrichtung auftreten, die das jeweilige Identitätsmerkmal der haltenden Person verwenden kann. Diese Rolle wird auch als „Prüfer" oder „Verifier" bezeichnet. In Bezug auf Identitätsmerkmale, die „Informationen zur Person" betreffen, kann das bspw. ein Hotel sein, in das die haltende Person eincheckt.[9] Auch Kreditinstitute können in der Rolle der verifizierenden Organisation auftreten. Das ist in Bezug auf das Identitätsmerkmal „Informationen zur Person" bspw. bei der Begründung einer Geschäftsbeziehung der Fall, für die die interessierte Person geldwäscherechtlich identifiziert werden muss.

d) Lizenzgebende Organisation

In der praktischen Anwendung des SSI-Konzepts kommt typischerweise eine vierte Rolle hinzu, nämlich die des Unternehmens, das als lizenzgebende Organisation die SSI-Wallet App anbietet: Die SSI-Wallet App dient v. a. natürlichen Personen in ihrer Rolle als haltende Personen dazu, die ihre Identität betreffenden Merkmale auf ihrem Smartphone zu verwalten. Das SSI-Konzept kann mit SSI-Wallet Apps unterschiedlicher Unternehmen genutzt werden. Am Markt gibt es SSI-Wallet Apps von Unternehmen mit privater und mit öffentlicher Eigentümerstruktur. Die Unternehmen

und die haltenden Personen schließen typischerweise über den App-Store (iOS) oder den Play Store (Android) einen Nutzungsvertrag („Lizenz") in Bezug auf die Nutzung der App.

e) eID, Smart-eID, Basis-ID

Aus der Sicht der geldwäscherechtlich „Verpflichteten" (§ 2 Abs. 1 GwG) ist für die Nutzung von SSI-Netzwerken besonders relevant, dass die haltenden Personen Merkmale über ihre Identität teilen können, die den Anforderungen des GwG genügen. Für die Zwecke dieses Beitrags wird der Fokus auf die drei hier sog. „Identitätsvarianten" „eID", „Smart-eID" und „Basis-ID" gerichtet. Ihre Integration in das „Ökosystem Digitale Identitäten", das das Projekt der Bundesregierung seit Ende 2020 aufbaut und das für geldwäscherechtlich Verpflichtete von besonderer Bedeutung ist, ist Gegenstand technischer und politscher Debatten.[10] Insbesondere die Vereinbarkeit dieser Identitätsvarianten mit den Leitmotiven von SSI und die IT-Sicherheit sind zwischen den diversen Akteuren umstritten.[11] Die technische Entwicklung der Smart-eID und der Basis-ID ist zudem noch nicht abgeschlossen. Einzelheiten werden zur Reduktion der Komplexität unten im Kontext der geldwäscherechtlichen Zulässigkeit der Nutzung der „Identitätsvarianten" dargestellt.[12]

2. GwG-Verpflichtete als verifizierende Organisationen

Die haltende Person kann mit ihrer SSI-Wallet App Angaben an die verifizierende Organisation übermitteln, wenn diese die Angaben für eine geldwäscherechtliche Identifizierung erheben muss. Im Massenverkehr trifft das insbesondere auf Kreditinstitute zu (§ 2 Abs. 1 Nr. 1 GwG). Daneben sind in bestimmten Fällen bspw. auch Rechtsanwälte und Notare (§ 2 Abs. 1 Nr. 10 GwG) oder, je nach Transaktionsgegenstand oder -wert, auch Güterhändler, Kunstvermittler und Kunstlagerhalter (§§ 2 Abs. 1 Nr. 16, 10 Abs. 6a GwG) zur Identifizierung verpflichtet. Die geldwäscherechtlich Verpflichteten treten in diesem Fall in der Rolle der verifizierenden Organisation auf. Zu diesem Zweck senden sie nach der Initiierung des Vorgangs durch die haltende Person eine Anfrage an deren SSI-Wallet App. Von der SSI-Wallet App werden nach der Freigabe durch die haltende Person sodann die Angaben an die verifizierende Organisation gesendet. In dem Fall, den der Gesetzgeber bei der Einführung der „Experimentierklausel" in § 13 GwG fördern wollte, werden die erheblichen Vorteile der Einbindung von SSI für die haltende Person und die verifizierende Organisation deutlich: Der Gesetzgeber bezweckte die Förderung der Einbindung von SSI durch Kreditinstitute in ihre Prozesse für die Online-Kontoeröffnung.[13] Die Übermittlung von Angaben „per Klick" in der SSI-Wallet kann in diesen Prozessen nicht nur die fehleranfällige und langwierige Eingabe der Information „per Hand" zu Beginn der „Klickstrecke" ersetzen. Zugleich entfällt die typischerweise am Ende der „Klickstrecke" stehende Überprüfung der eingegebenen Daten, etwa per Videoverfahren, Filiale oder Post. Die Dauer des gesamten Prozesses der Kontoeröffnung inklusive Identifizierung kann dadurch auf drei Minuten reduziert werden.[14] Die Verarbeitung der Angaben der haltenden Person im Kernbanksystem des Instituts läuft nach der Erhebung technisch dann genauso ab, wie in anderen Fällen der Erhebung, etwa beim Vorzeigen des Personalausweises in der Filiale.

III. Geldwäscherechtliche zulässige Identifizierung anhand von SSI-Identitäten

Die nachfolgenden Betrachtungen werden am Beispiel von Kreditinstituten als GwG-Verpflichtete vorgenommen. Sie lassen sich sinngemäß auf andere GwG-Verpflichtete übertragen.

1. Überblick: „Zweiaktiges" Identifizierungsverfahren des GwG

Institute sind gemäß § 2 Abs. 1 Nr. 1 GwG „Verpflichtete" nach dem GwG. Als solche haben Sie ihre Vertragspartner zu identifizieren, indem sie ein zweiaktiges Verfahren durchführen – die

Erhebung von Angaben über die Person und die Überprüfung der Angaben (§ 11 Abs. 1 S. 1 GwG). Der Gesetzgeber spricht in Bezug auf die zwei Vorgänge explizit von „Teilakten".[15] Das wirft die Frage auf, ob Erhebung und Überprüfung auch zusammenfallen

können. Denn das geschieht bei der Nutzung eines SSI-Identitätsnachweises, indem ein schon geprüfter Identitätsdatensatz erhoben wird.[16] Eine Trennung zwischen Erhebung und Überprüfung der Angaben widerspräche dem SSI-Konzept. Das GwG enthält keinen Grundsatz, nach dem die Teilakte nicht zusammenfallen dürfen. Im Gegenteil: In § 17 Abs. 3a GwG sieht der Gesetzgeber mit der sog. „Wiederverwertung" die Übernahme eines nach dem GwG geprüften Identitätsdatensatzes von einem Dritten sogar explizit vor. Warum die Nutzung von SSI keine Wiederverwertung in diesem Sinne ist, wird unten dargestellt.[17] Die Existenz der „Wiederverwertung" genügt an dieser Stelle, um zu zeigen, dass die Zusammenführung von Erhebung und Überprüfung bei der Nutzung von SSI nicht per se im Widerspruch zum GwG steht. Entscheidend ist, dass dieser „eine" Akt die Anforderungen des GwG an die Teilakte „Erhebung" und „Überprüfung" erfüllt:

2. Erster Teilakt: Erhebung von Angaben

Gemäß § 11 Abs. 4 Nr. 1 GwG sind von einer natürlichen Person die folgenden Angaben zu erheben: a) Vorname und Nachname, b) Geburtsort, c) Geburtsdatum, d) Staatsangehörigkeit und e) eine Wohnanschrift oder in bestimmten Fällen eine postalische Anschrift. Wie die Erhebung der Angaben von der haltenden Person vonstatten zu gehen hat, hängt davon ab, welchen Identitätsnachweis sie verwendet. Beim physischen Personalausweis kann der Erhebungsvorgang bspw. im Abschreiben oder Auslesen der Daten liegen. Bei elektronischen Identitätsnachweisen werden die Angaben durch Datenübertragung erhoben. Auch die Erhebung der Angaben über ein SSI-Netzwerk kommt damit als zulässige Erhebungsform in Betracht.

3. Zweiter Teilakt: Überprüfung erhobener Angaben nach § 12 GwG

a) Überblick

Nach § 12 Abs. 1 S. 1 GwG sind die erhobenen Angaben grundsätzlich anhand eines der Nachweise zu überprüfen, die in § 12 Abs. 1 S. 1 Nr. 1 bis 5 GwG aufgelistet sind. Ein SSI-Identitätsnachweis müsste sich also grundsätzlich einem der dort genannten Nachweise zuordnen lassen, um den Anforderungen des GwG an die Überprüfung zu genügen. Nach § 12 Abs. 1 S. 1 Nr. 2 GwG kann die Überprüfung der erhobenen Angaben u. a. *„anhand […] eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes*" erfolgen. Verifizierende Organisationen haben daher zunächst zu prüfen, ob der SSI-Identitätsnachweis, den sie entgegennehmen wollen, ein elektronischer Identitätsnachweis in diesem Sinne ist. Um diese Frage beantworten zu können, muss der Blick vom abstrakten Begriff der SSI-Identitätsnachweise gelöst und auf die tatsächlich praktisch diskutierten[18] Identitätsvarianten gerichtet werden: eID, Smart-eID und Basis-ID.

b) eID, Smart-eID, Basis-ID – Einzelheiten

eID, Smart-eID und Basis-ID sind elektronische Identitätsnachweise, die die Angaben enthalten, die Verpflichtete nach dem GwG erheben und prüfen müssen (Vorname und Nachname, Geburtsort, Geburtsdatum, Staatsangehörigkeit, Wohnanschrift). Die „Identitätsvarianten" unterscheiden sich allerdings in ihrer IT-Architektur:

Die eID hebt sich von der Smart-eID und der Basis-ID zunächst dadurch ab, dass sie nur in Kombination mit der Ausweiskarte eingesetzt werden kann. Die Ausweiskarte enthält auf einem Chip die Identitätsnachweise. Der Chip muss bei jedem elektronischen Identifizierungsvorgang ausgelesen werden. Zu beachten ist, dass die Abhängigkeit von dem Chip zu einer „Lösung" von einem der Grundprinzipien des SSI-Konzepts führt. Die haltende Person soll die Hoheit über die Nachweise haben, bspw. in einer Wallet-App. Bei der eID bleibt der Nachweis dagegen auf der Karte. Deshalb spielt die „klassische" eID bei der Diskussion um die Entwicklung eines SSI-Ökosystems im Projekt „Ökosystem Digitale Identitäten" eine untergeordnete Rolle.[19]

Parallel zur Einfügung der Experimentierklausel in § 13 GwG (und derzeit andauernd) wurde die eID weiterentwickelt zur sog. Smart-eID.[20] Dabei handelt es sich um eine Möglichkeit, den Online-Ausweis auf dem Smartphone zu speichern, sodass der Identitätsnachweis ohne Ausweiskarte genutzt werden kann. Das kommt dem SSI-Konzept näher. Kritisiert wird[21], dass die Speicherung in der aktuellen Version der Smart-eID nur in einem physischen sog. „Secure Element" im Smartphone erfolgt. Das ist ein speziell abgeschirmter Chip, der in vielen Smartphones vorhanden ist. Stand heute ist dieses Secure Element aber nur in einer Gerätereihe von Samsung durch den Hersteller für die Smart-eID freigegeben,[22] sodass die Reichweite der Smart-eID begrenzt ist. Das Bundesministerium des Innern (BMI) arbeitet daran, die Zahl der unterstützen Geräte und damit die Reichweite der Smart-eID zu erhöhen.[23] Eine Erhöhung der Reichweite wäre auch möglich, indem die Smart-eID auf das Secure Element verzichtet und so weiterentwickelt wird, dass sie mit anderen Sicherheitschips[24] in Smartphones funktioniert, auf die ohne Freigabe des Herstellers zugegriffen werden kann.[25]

Die Basis-ID unterscheidet sich von der Smart-eID dadurch, dass sie direkt in der SSI-Wallet App gespeichert und von dort zugänglich gemacht werden kann.[26] Vorgesehen ist, dass ein Register gesperrter Informationen und Informationen über die ausstellende Organisation (public keys) über eine DLT zugänglich gemacht werden.[27] Die Basis-ID spielt bei vielen Anwendungsfällen des Projekts „Ökosystem Digitale Identitäten" eine Rolle.[28] Auch ihre technische Entwicklung ist noch nicht abgeschlossen. Soweit erkennbar,[29] ist in der IT-Infrastruktur, die die Basis-ID nutzt, zum Zeitpunkt der

Veröffentlichung dieses Beitrags noch nicht vorgesehen, dass sich die verifizierende Organisation gegenüber der haltenden Person als zur Entgegennahme des Identitätsnachweises „berechtigt" zu erkennen geben muss („Berechtigungszertifikat"). Das bedeutet, dass die haltende Person nicht sicher weiß, ob sie ihre Daten an eine zum Erhalt berechtigte Stelle übermittelt. Das und die Nutzung von DLT unterscheidet die Bereitstellung der Basis-ID von der Bereitstellung der eID und der Smart-eID derzeit.

c) Geldwäscherechtliche Bewertung der Eigenschaften

Nach § 12 Abs. 1 S. 1 Nr. 2 GwG kann die Überprüfung der erhobenen Angaben u. a. *„anhand […] eines elektronischen Identitätsnachweises nach § 18 des Personalausweisgesetzes*" erfolgen. Die Neu-Fassung von § 18 PAuswG ist am 1. September 2021 in Kraft getreten. Er erfasst zwei der drei vorgestellten „Identitätsvarianten".

aa) eID zulässig

Nach § 18 Abs. 2 S. 1 Nr. 1 PAuswG gilt: *„Der elektronische Identitätsnachweis erfolgt durch Übermittlung von Daten 1. aus dem elektronischen Speicher- und Verarbeitungsmedium des*

Personalausweises […]". Das legitimiert die Nutzung der eID. Denn das „Speicher- und Verarbeitungsmedium des Personalausweises" ist der Chip auf der Ausweiskarte, auf dem die eID-Daten gespeichert sind. Nach § 18 Abs. 4 S. 1 PAuswG hat die verifizierende Organisation vor der Entgegennahme des Identitätsnachweises an die haltende Person ein Berechtigungszertifikat zu übermitteln. Das wird im Rahmen der eID-Infrastruktur von der Bundesdruckerei ausgestellt.[30] Allerdings bleibt zu betonen, dass die eID aufgrund der Bindung an die Ausweiskarte nur schwer für den Einsatz in einem Wallet-basierten SSI-Ökosystem verwendbar ist. Die Bedeutung der geldwäscherechtliche ohne Weiteres verwendbaren eID für SSI-Ökosysteme dürfte daher gering bleiben.

bb) Smart-eID zulässig

Nach § 18 Abs. 2 S. 1 Nr. 2 PAuswG gilt seit dem 1. September 2021: „*Der elektronische Identitätsnachweis erfolgt durch Übermittlung von Daten […] 2. aus einem elektronischen Speicher- und Verarbeitungsmedium in einem mobilen Endgerät*". Damit ist nach der Gesetzesänderung im September 2021 auch die Smart-eID erfasst. Denn das physische Secure Element im Smartphone kann ein „Speicher- und Verarbeitungsmedium in einem mobilen Endgerät" darstellen, auf dem die Smart-eID-Informationen gespeichert sind. Auch bei der Nutzung der Smart-eID hat nach § 18 Abs. 4 S. 1 PAuswG die verifizierende Organisation vor der Entgegennahme des Identitätsnachweises an die haltende Person ein Berechtigungszertifikat zu übermitteln. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) geht in der letzten veröffentlichten Entwurfsfassung seines Leitfadens zur Integration der Smart-eID davon aus, dass dies wie bei der eID abgewickelt werden kann.[31]

Ob auch eine weiterentwickelte Version der Smart-eID, die auf das Secure Element verzichtet[32], den Vorgaben von § 18 Abs. 2 S. 1 Nr. 2 PAuswG entsprechen kann, ist offen. Obwohl das aus dem Wortlaut und der Gesetzesbegründung nicht eindeutig hervorgeht,[33] geht das BSI in Veröffentlichungen zur Änderung von § 18 PAuswG davon aus, dass der Speicher den höheren technischen Anforderungen an ein Secure Element genügen muss.[34] Dabei legt es das bisher verbreitete Verständnis des Begriffs als physischer, gesonderter Chip auf dem Gerät zugrunde.[35] Systeme, die auf Secure Elements verzichten, entsprächen diesem Begriffsverständnis nicht. Wenn sich dieses Verständnis durchsetzte, schiede § 18 Abs. 2 S. 1 Nr. 2 PAuswG als Anknüpfungspunkt für die weiterentwickelte Smart-eID aus. Anderenfalls wäre diese Innovation ohne Rückgriff auf die Experimentierklausel nutzbar.

cc) Zulässigkeit der Basis-ID offen

Ob die Basis-ID den Anforderungen von § 18 Abs. 2 S. 1 Nr. 2 PAuswG entspricht, kann in Anbetracht ihrer noch offenen technischen Entwicklung noch nicht abschließend bewertet werden. Entscheidend ist auch hier, ob die Basis-ID und die technische Infrastruktur, in der sie verwendet werden soll, die Anforderungen an die Beschaffenheit des Speichers des Smartphones erfüllen (§ 18 Abs. 2 S. 1 Nr. 2 PAuswG) und ob die verifizierende Organisation ihre Berechtigung zum Erhalt der Daten gegenüber der haltenden Person hinreichend belegen kann (§ 18 Abs. 4 S. 1 PAuswG).

Die Speicherung der Daten in der App führt dazu, dass die Daten auch auf dem Speicher des verwendeten Smartphones gespeichert werden. Ob ihre Übermittlung aus einer SSI-Wallet App damit auch eine Übermittlung „aus einem elektronischen Speicher- und Verarbeitungsmedium in einem mobilen Endgerät" nach § 18 Abs. 2 S. 1 Nr. 2 PAuswG darstellt, ist fraglich. Wie soeben gesehen, geht das BSI davon aus, dass der Speicher den höheren technischen Anforderungen an ein Secure Element genügen müsse und deshalb der allgemeine Speicher des Smartphones wohl

nicht genüge.[36] Bei der Bewertung einer künftigen Weiterentwicklung der Basis-ID wird, wie auch bei der Bewertung einer weiterentwickelten Version der Smart-eID, die auf das Secure Element verzichtet, der Umstand eine Rolle spielen, dass ein erhöhtes Sicherheitsniveau nicht nur über ein Secure Element, sondern auch über Software und Hardware-Komponenten gewährleistet werden kann, deren Nutzung nicht von Freigaben der Hersteller abhängt. Dann wäre ein Secure Element nicht erforderlich.

Auch bei der Nutzung der Basis-ID hat nach § 18 Abs. 4 S. 1 PAuswG die verifizierende Organisation vor der Entgegennahme des Identitätsnachweises an die haltende Person ein Berechtigungszertifikat zu übermitteln. Das ist, soweit bekannt, in der aktuellen technischen Entwicklungsphase noch nicht vorgesehen. Dieser Umstand hat im Rahmen des Anwendungsfalles „Digitaler Führerschein" des Projekts „Ökosystem Digitale Identitäten" zu Kritik geführt.[37] Bei einer entsprechenden Weiterentwicklung der Basis-ID könnte die Bereitstellung eines entsprechenden Zertifikats berücksichtigt werden. Dann käme die Entsprechung der Basis-ID mit den Anforderungen von § 18 Abs. 4 S. 1 PAuswG in Betracht. In diesem Fall wäre, bei hinreichend abgesichertem Speicher, auch vertretbar, sie als Identitätsnachweis im Sinne von § 18 Abs. 2 S. 1 Nr. 2 PAuswG einzustufen. Dann kann sie auch einen Identitätsnachweis im Sinne von § 12 Abs. 1 S. 1 Nr. 2 GwG darstellen.

d) Zielkonflikt zwischen Sicherheit und Nutzbarkeit?

Die eID wird wegen der Ausweiskarte und die Smart-eID aufgrund der geringen Verbreitung von nutzbaren Secure Elements auf Smartphones von vielen Marktteilnehmern abgelehnt. Das BMI plant gleichwohl mit der Smart-eID weiter.[38] Die Basis-ID findet dagegen hohe Akzeptanz auf Seiten der Marktteilnehmer.[39] Gleiches könnte für eine weiterentwickelte Version der Smart-eID, die auf das Secure Element verzichtet und deshalb eine höhere Reichweite hätte, gelten. Ob sich daraus ein Zielkonflikt zwischen Sicherheit und Nutzbarkeit ergibt, hängt davon ab, ob die Basis-ID oder die weiterentwickelte Smart-eID ein GwG-konformer Identitätsnachweis sein können, obwohl sie Stand heute noch nicht sicher von § 12 Abs. 1 GwG erfasst sind. Das erscheint zumindest nach den geldwäscherechtlichen Rahmenbedingungen insoweit möglich, als § 12 GwG die zulässigen Identitätsnachweise nicht abschließend aufzählt. Stattdessen kann die Überprüfung der Angaben mittels Basis-ID oder Smart-eID, die auf das Secure Element verzichtet, auch nach § 13 GwG möglich sein.

e) § 13 GwG als Ergänzung von § 12 GwG

§ 13 Abs. 1 Nr. 1 und 2 GwG nennen die Verfahren, mit denen anhand bestimmter Nachweise die Identität überprüft wird, nämlich: Augenscheinnahme (Nr. 1) und sonstiges gleichwertiges Verfahren (Nr. 2). Das Verhältnis von § 13 Abs. 1 GwG zu § 12 Abs. 1 GwG erschließt sich nicht auf den ersten Blick. Der Gesetzgeber (in der Gesetzesbegründung[40]) und die BaFin (in ihren AuA[41]) sprechen aber klar aus, dass die Nachweise des § 12 Abs. 1 S. 1 Nr. 2 bis 5 GwG andere geeignete Verfahren sind, die ein gleichwertiges Sicherheitsniveau aufweisen. Das bedeutet, dass die Verfahren nach § 12 die Anforderungen von § 13 Abs. 1 Nr. 2 GwG erfüllen. Alle Verfahren nach § 12 Abs. 1 S. 1 Nr. 2 bis 5 GwG sind also Verfahren im Sinne von § 13 Abs. 1 Nr. 2 GwG. Wenn die Liste von § 12 Abs. 1 S. 1 GwG abschließend wäre, wäre § 13 Abs. 1 Nr. 2 GwG aber überflüssig. Die Liste des § 12 konkretisiert § 13 Abs. 1 Nr. 2 GwG also nicht abschließend.[42] § 13 Abs. 1 Nr. 2 GwG öffnet stattdessen den starren Nachweis-Katalog von § 12 Abs. 1 S. 1 Nr. 1

bis 5 GwG für sonstige Verfahren, die nicht in diesem Katalog stehen – unter der Voraussetzung, dass sie „gleichwertig" zur Augenscheinnahme sind.

f) Die Experimentierklausel im Gefüge von § 12 und 13 GwG

Der Gesetzgeber hat die „Offenheit" von § 13 Abs. 1 Nr. 2 GwG zur Unterstützung der SSI-Strategie der Bundesregierung um eine „Experimentierklausel" ergänzt. Mit der Klausel erhalten das Bundesministerium der Finanzen (BMF), das BMI und Behörden (BSI und BaFin) die Gelegenheit zur Mitwirkung in der Phase der Erprobung von SSI. Verpflichtete erhalten die Gelegenheit, Verfahren einzusetzen, deren „Gleichwertigkeit" mit der Augenscheinnahme noch nicht festgestellt wurde.

Da der Gesetzgeber die Experimentierklausel explizit zur Förderung von SSI in das GwG aufgenommen hat, liegt es zunächst nahe, danach zu fragen, ob und unter welchen Voraussetzungen die Nutzung der Basis-ID und sonstiger ID-Alternativen, wie etwa einer weiterentwickelten Smart-eID, die auf ein Secure Element verzichtet, auf die Experimentierklausel gestützt werden kann. In Bezug auf die eID und die Smart-eID mit Secure Element ist die Experimentierklausel dagegen irrelevant. Denn beide Verfahren sind nach der in zeitlicher Hinsicht parallel[43] zur Einführung der Experimentierklausel erfolgten Anpassung des PAuswG bereits nach § 12 Abs. 1 S. 1 Nr. 2 GwG iVm § 18 PAuswG zulässig[44].

Im nächsten Abschnitt wird zunächst gezeigt, dass es grundsätzlich möglich ist, die Nutzung der Basis-ID und der „Software Smart-eID" auf die Experimentierklausel zu stützen. Sodann wird dargestellt, dass die Standpunkte des BSI die Nutzung der Basis-ID, wenn überhaupt, in einem maximal reduzierten Sandbox-Ansatz erzwingen. Deshalb folgt im Anschluss die Darstellung der abstrakt bestehenden Möglichkeit, die Basis-ID unabhängig von der Experimentierklausel zur Erhebung geprüfter Angaben zu nutzen.

4. Überprüfung nach § 13 GwG „mit Experimentierklausel"

Gemäß § 13 Abs. 2 S. 1 Nr. 3, S. 2 und 3 GwG muss ein Identifizierungsverfahren drei formelle Voraussetzungen erfüllen, um vom Institut zur Identifizierung im Rahmen der sog. „Experimentierklausel" verwendet werden zu können: (1) Bestimmung des Verfahrens durch BMF und BMI in einer Verordnung, (2) Feststellung der Sicherheit durch das BSI und (3) Zulassung durch die BaFin. Im Einzelnen:

a) Bestimmung des Verfahrens durch BMF und BMI

Gemäß § 13 Abs. 2 S. 1 Nr. 3 GwG kann das BMF „im Einvernehmen mit" dem BMI Verfahren bestimmen, deren Eignung zur geldwäscherechtlichen Überprüfung der Identität erprobt wird. Die Betonung der „Überprüfung" ist insoweit bemerkenswert, als die SSI-Technologie nicht nur zur Überprüfung dient. Einen erheblichen praktischen Mehrwert liefern die ID-Wallets, weil sie auch die Erhebung der Daten vom Kunden ermöglichen. Beides, Erhebung und Überprüfung, wird in einem Vorgang vollzogen. Die Identitätsnachweise werden „überprüft erhoben".[45] Zum Zeitpunkt der Erstellung dieses Beitrags hat der Verordnungsgeber von seiner Kompetenz noch keinen Gebrauch gemacht. Ob er das künftig tun wird, ist angesichts der noch andauernden technischen Entwicklung von Basis-ID und Smart-eID sowie der zweiten Voraussetzung für die Nutzung eines Verfahrens auf der Grundlage der Experimentierklausel offen:

b) Feststellung des notwendigen Sicherheitsniveaus durch das BSI

aa) Positionen des BSI zu SSI, DLT und Basis-ID

Gemäß § 13 Abs. 2 S. 3 GwG muss das BSI vor der Zulassung durch die BaFin feststellen, dass das in der Verordnung geregelte Verfahren zur Erprobung von SSI „das für die Erprobung notwendige Sicherheitsniveau" aufweist. Im Hinblick darauf, welchen „Effekt" die Experimentierklausel haben kann, ist zunächst bemerkenswert, dass das BSI seine erhebliche Kritik an der Sicherheitsarchitektur hinter der praktisch für den Fall der Erprobung besonders relevanten Basis-ID schon konkretisiert hat, bevor sein „Votum" als Voraussetzung der Experimentierklausel in das GwG aufgenommen wurde. Der Finanzausschuss hat die Einfügung der

Experimentierklausel (samt der Befugnisse des BSI) in den entsprechenden Gesetzesentwurf Anfang Juni 2021 empfohlen.[46] Der Bundestag hat die entsprechend geänderte Fassung sodann am 25. Juni 2021 beschlossen, die Änderung trat am 1. August 2021 in Kraft.[47] Aber bereits vor der Empfehlung des Finanzausschusses hat das BSI am 11. Mai 2021 erhebliche Sicherheitsbedenken gegen die Infrastruktur der Basis-ID in der damaligen technischen Konfiguration formuliert.[48] Parallel zu dieser Entwicklung hat der Gesetzgeber zudem durch eine Anpassung des PAuswG[49] die Voraussetzungen dafür geschaffen, dass die Smart-eID GwG-konform[50] genutzt werden kann.

Ohne dass mittlerweile ein Verordnungsentwurf des BMF oder eine Aufforderung der BaFin bekannt geworden ist, hat sich das BSI Ende 2021 erneut zur Sicherheit in SSI-Infrastrukturen geäußert – in diesem Fall ohne konkreten Bezug zu einem der Anwendungsfälle des Projekts „Ökosystem Digitale Identitäten".[51] Bei der Auseinandersetzung mit dieser Äußerung des BSI ist gleichwohl zu berücksichtigen, dass die Basis-ID und die dazugehörige IT-Infrastruktur vorsieht, dass ein Register gesperrter Informationen und Informationen über die ausstellende Organisation (public keys) über eine DLT zugänglich gemacht werden.[52] In seiner neueren Stellungnahme erteilt das BSI dem eine klare Absage. Das BSI erläutert, dass es das notwendige Sicherheitsniveau in einem SSI-Netzwerk nicht für gegeben hält, wenn die technische Infrastruktur eines SSI-Netzwerks auch DLT einbezieht.[53] DLT sei u. a. geprägt von fehlenden Standards und einem Mangel an etablierten Sicherheitsempfehlungen. Protokolle und kryptografische Verfahren seien wenig untersucht. Standardisierungsprozesse seien nicht abgeschlossen. Damit ist klar: Auf die Experimentierklausel wird der aktuelle Ansatz zur Bereitstellung der Basis-ID oder die Nutzung einer sonstigen ID-Alternative nur in drei Fällen gestützt werden können: erstens, wenn die technische Infrastruktur der Basis-ID weiterentwickelt wird aber die Weiterentwicklung *noch nicht* so weit geht, dass sich die Zulässigkeit bereits aus § 12 Abs. 1 S. 1 Nr. 2 GwG ergibt[54]; zweitens, wenn eine weiterentwickelte Version der Smart-eID zum Einsatz kommt, die wegen des Verzichts auf das Secure Element *nicht mehr* den Anforderungen § 12 Abs. 1 S. 1 Nr. 2 GwG entspricht; drittens, wenn bei gleichbleibender Technologie die Erprobung so sehr eingeschränkt wird, dass das BSI trotz seiner grundlegenden Bedenken das (dann niedrigere) notwendige Sicherheitsniveau feststellen kann. Die ersten beiden Fälle hängen von der Weiterentwicklung der (staatlichen) Infrastruktur ab, der dritte von den anwendenden Unternehmen:

bb) Beschränkung der Erprobung

Dass eine Beschränkung der Erprobung die Nutzung der Basis-ID und sonstiger ID-Alternativen ermöglichen kann, ist in der Experimentierklausel angelegt: § 13 Abs. 2 S. 3 GwG fordert kein allgemein hohes Sicherheitsniveau, sondern das „für die Erprobung" notwendige. Die beteiligten Organisationen haben es über die Bezugsgröße „Erprobung" damit selbst in der Hand, wie hoch

das Sicherheitsniveau sein muss, das das BSI als ausreichend feststellen soll. Zwischen dem Betrieb in einer Testumgebung einerseits und einem uneingeschränkten Live-Betrieb ist viel Raum für das, was als „Erprobung" in Betracht kommt. Parameter, die das notwendige Sicherheitsniveau absenken, können vor allem in selbst auferlegten Beschränkungen liegen, etwa Beschränkungen der Dauer der Erprobung, der Kundengruppen, der Kundenzahlen oder der durchführbaren Geschäfte, insoweit v. a. die Wahl zwischen bestandverändernden und nicht-bestandsverändernden Geschäften. Das BSI hat Einschränkungen dieser Art für die Erprobung im Anwendungsfall „Hotel-Check-In" für tauglich erachtet, um eine Erprobung trotz Bedenken gegen die Sicherheit der Nutzung der Basis-ID durchzuführen.[55] Die im Hotel-Bereich weniger wichtige aber für Anwendungsfälle aus dem Finanzsektor umso relevantere „Stellschraube" der Beschränkung auf nicht-bestandverändernde Geschäfte erscheint besonders sinnvoll, um finanzielle Risiken für die Beteiligten zu senken. Diese Beschränkung ist aber schwer vereinbar mit den Ambitionen des Gesetzgebers. Nach der Gesetzesbegründung ging es ihm gerade darum, die „Kontoeröffnung bei Verpflichteten nach § 2 Abs. 1 Nummer 1" zu ermöglichen – also einen Vorgang, der bestandsverändernde Folgen haben kann.[56]

cc) Berücksichtigung der Privilegierung

Die Einschränkung der Erprobung eines Verfahrens durch eine Begrenzung der Kundengruppen (keine Neukunden) und der Geschäftsarten (keine Bestandveränderung) kann dazu führen, dass das GwG auf den Fall, in dem das Verfahren erprobt werden würde, gar nicht mehr anwendbar ist. Dann ginge die privilegierende Wirkung[57] der Experimentierklausel verloren. Insoweit können die Beteiligten, die die Experimentierklausel nutzen wollen, bei ihrer „Selbstbeschränkung" beachten, dass sie das Risiko ihres Verfahrens nicht auf „null" senken müssen. § 13 Abs. 2 Nr. 3 GwG stellt nämlich fest, dass die Verfahren, die per Verordnung zugelassen werden können, gerade Verfahren sind, von denen noch nicht feststeht, *„ob sie ein Sicherheitsniveau aufweisen, das dem in Absatz 1 Nummer 1 genannten Verfahren gleichwertig ist.*" Das jeweilige Verfahren muss also mindestens das „für die Erprobung notwendige Sicherheitsniveau" aufweisen (Abs. 2 Nr. 3) aber es muss deshalb noch kein mit der Inaugenscheinnahme gleichwertiges Sicherheitsniveau erreichen. Das zu erreichende Sicherheitsniveau ist also niedriger als das der „Gleichwertigkeit", die § 13 Abs. 1 Nr. 2 GwG für alternative Verfahren fordert. Die privilegierende Wirkung der Experimentierklausel kann deshalb nicht nur die Verwendung der Basis-ID mit verbesserter Infrastruktur ermöglichen. Möglich erscheint auch, dass die Nutzung einer weiterentwickelten Variante der Smart-eID, die wegen des Verzichts auf das in nur wenigen Geräten vom Hersteller freigegebene Secure Element nach Auffassung des BSI nicht mehr den Anforderungen von § 18 PAuswG entspricht, auf die Experimentierklausel gestützt werden kann.

c) Zulassung der BaFin

Gemäß § 13 Abs. 2 S. 2 GwG können die Aufsichtsbehörden nach § 50 GwG die Nutzung des Verfahrens zulassen, wenn a) die Verordnung von BMF und BMI sie dazu ermächtigt und b) das BSI das „zur Erprobung notwendige Sicherheitsniveau" festgestellt hat. Die für Institute zuständige Aufsichtsbehörde ist nach § 50 Nr. 1 GwG die BaFin. Ob die Voraussetzungen dafür, dass die BaFin von ihrem Recht zur Zulassung Gebrauch machen kann, eintreten, ist im Hinblick auf die Stellungnahmen des BSI offen – siehe zuvor.

5. Überprüfung nach § 13 GwG „ohne Experimentierklausel"

a) „Ex-post"-Betrachtung der Gleichwertigkeit zulässig

Selbst wenn ein neues Identifizierungsverfahren genutzt wird, ohne dass die Voraussetzungen der Experimentierklausel erfüllt sind, ist das nicht per se gleichzusetzen damit, dass das Identifizierungsverfahren geldwäscherechtlichen Anforderungen nicht genügen kann. Das Konzept der Experimentierklausel folgt dem Ansatz, ex ante festzustellen, ob ein Identifikationsverfahren „das für die Erprobung notwendige Sicherheitsniveau" hat. Der Wortlaut von § 13 Abs. 2 S. 3 GwG ist in Bezug auf die Erprobung insoweit eindeutig, als die Zulassung des BSI nur erfolgt, wenn es bei „einer vorherigen Überprüfung" die Sicherheit festgestellt hat.

Aus dem Wortlaut von § 13 GwG und seinem Sinn und Zweck ergibt sich aber, dass die hinreichende Sicherheit außerhalb von Erprobungen auf der Grundlage der Experimentierklausel auch ex post festgestellt werden kann – wenn das Verfahren schon im Einsatz ist und ohne dass es auf einer Verordnung nach § 13 Abs. 2 S. 1 Nr. 2 GwG beruht, die die „Gleichwertigkeit" bestimmt. Die Kernaussage von § 13 Abs. 1 GwG lautet: Prüfe die Angaben durch Inaugenscheinnahme (Nr. 1) oder prüfe sie durch ein sonstiges Verfahren, das gleichwertig ist (Nr. 2). Von der Anforderung an den Verpflichteten, eine Inaugenscheinnahme durchzuführen oder ein sonstiges gleichwertiges Verfahren zu nutzen, rückt Abs. 2, auch nachdem die Experimentierklausel eingeführt wurde, nicht ab. Nach dem Wortlaut von § 13 Abs. 2 GwG sind weder die Verordnung, die das BMF erlassen kann, noch die Feststellung des BSI, noch die Zulassung der BaFin Voraussetzung für die Überprüfung von Angaben mittels eines sonstigen gleichwertigen Verfahrens. Stattdessen „kann" das BMF nach Abs. 2 eine Verordnung erlassen, in der es „Konkretisierungen oder Anforderungen" festlegt (Nr. 1) oder Verfahren bestimmt, die als „gleichwertig" geeignet sind (Nr. 2) oder Verfahren bestimmt, die erprobt werden (Experimentierklausel gemäß Nr. 3 und S. 2 und 3). Der Wortlaut von Abs. 2 enthält keinen Anhaltspunkt dafür, dass die Regelung von Möglichkeiten zum Tätigwerden per Verordnung zugleich die Entscheidung von Verpflichteten sperren soll, Verfahren ohne Verordnung einzusetzen. Die Position der BaFin zu der Frage, ob es neben Verfahren, die in Verordnungen geregelt sind, noch Raum für Verfahren geben kann, die ohne Verordnung genutzt werden dürfen, kann nicht eindeutig bestimmt werden. In der alten und der aktualisierten Fassung ihrer Auslegungs- und Anwendungshinweise zum GwG führt die BaFin einerseits aus, sonstige gleichwertige Verfahren könnten „ausschließlich durch Rechtsverordnung" zugelassen werden.[58] Andererseits ist die BaFin aber mit ihrem Rundschreiben 3/2017 selbst einen anderen Weg gegangen. In dem Rundschreiben beschreibt sie die Anforderungen an die Videoidentifizierung als Variante der Kontrolle unter Anwesenden und bringt dadurch auch zum Ausdruck, dass es für den Einsatz eines alternativen Verfahrens gerade nicht auf eine (ministerielle) Rechtsverordnung ankommt.[59] *Frey* stellt zurecht fest, dass auch der Zweck von § 13 Abs. 2 GwG der Beschränkung auf die ex ante-Feststellung entgegensteht.[60] In der Begründung der ursprünglichen Fassung der Vorschrift, die die Experimentierklausel noch nicht enthielt, gibt der Gesetzgeber an, dass er dem Verordnungsgeber (BMF) Handlungsspielraum geben wollte: Der Verordnungsgeber könne „kurzfristig auf sich am Markt abzeichnende Entwicklungen neuer Identifizierungsverfahren reagieren und bestimmen, welche Verfahren […] generell als geeignet anzusehen sind".[61] Das geht aber erst, wenn das Verfahren schon im Einsatz ist.[62] Diesen Zweck reduziert der Gesetzgeber auch nicht in der Begründung der Experimentierklausel.[63] Ähnlich wie im Wortlaut der Norm („kann"), formuliert der Gesetzgeber in der Begründung, dass es dem Verordnungsgeber (BMF) nunmehr „erlaubt" ist, Verfahren zur Erprobung zuzulassen. Daraus, dass dem BMF eine Erlaubnis erteilt wird, eine Verordnung zu erlassen, werden Marktteilnehmer

aber nicht darin beschränkt, ihre Verfahren auch ohne das vorher per Verordnung erteilte exekutive Plazet einzusetzen.

b) Maßstab Gleichwertigkeit

Verifizierende Organisationen, die die Basis-ID oder sonstige ID-Alternativen zur geldwäscherechtlichen Überprüfung von Identitäten einsetzen wollen, müssen außerhalb des Freiraums, den die Experimentierklausel durch das abgesenkte Sicherheitsniveau für Erprobungen in ihrem Sinne gewährt, allerdings die volle „Gleichwertigkeit" des Verfahrens begründen können (§ 13 Abs. 1 Nr. 2 GwG). Als „Richtschnur" können ihnen dabei die nach § 12 Abs. 1 S. 1 Nr. 1 bis 5 GwG zugelassenen Verfahren dienen. Ob sie die Risiken des neuen Verfahrens und seine Nutzerfreundlichkeit (als Kriterien der „notwendigen Sicherheit") aber auf eigenes Risiko abwägen und sich in den Richtungskampf[64] der Ministerien verwickeln lassen, bleibt abzuwarten.

6. Zwischenergebnis

Damit ist festzuhalten: Die eID und die Smart-eID können in SSI-Netzwerken zur GwG-konformen Identifizierung von Personen genutzt werden. Denn ihre Nutzung ist gemäß § 12 Abs. 1 S. 1 Nr. 2 GwG iVm § 18 Abs. 2 S. 1 Nr. 1 und 2 PAuswG zulässig. Die Bindung der eID an die Ausweiskarte führt aber zu Widersprüchen mit SSI-Prinzipien. Die Smart-eID kann SSI-Prinzipien entsprechen. Sie ist in ihrer aktuellen Ausprägung am Markt aber kaum verfügbar, weil nur wenige Endgeräte ein nutzbares Secure Element haben. Die Identifizierung mit der Basis-ID kann derzeit nicht auf § 12 Abs. 1 S. 1 Nr. 2 GwG gestützt werden, weil sie die Anforderungen von § 18 PAuswG nicht erfüllt (u. a. Berechtigungszertifikat). Solange die Basis-ID im SSI-Ökosystem, das das Bundeskanzleramt und Ministerien derzeit aufbauen, auf DLT zurückgreift, wird sie voraussichtlich auch nicht auf der Grundlage der Experimentierklausel am Markt zu dem vorgesehenen Zweck „Kontoeröffnung" getestet werden können. Denn dafür wäre die Feststellung des notwendigen Sicherheitsniveaus durch das BSI erfor-

derlich. Das BSI hat aber bereits zu erkennen gegeben, dass es dieses Niveau unter Einbeziehung von DLT nicht für gegeben hält. Die Basis-ID und sonstige ID-Alternativen können aber grundsätzlich auch „außerhalb" der Experimentierklausel als sonstiges gleichwertiges Verfahren von Marktteilnehmern (auf eigenes Risiko) eingesetzt werden, denn § 13 GwG sperrt die „Ex-post"-Betrachtung der Sicherheit des Verfahrens nicht.

7. Notwendige „Annex-Erhebung" bei eID und Smart-eID

Aus den Aufzeichnungs- und Aufbewahrungspflichten nach § 8 Abs. 1 und 2 GwG ergibt sich, dass Verpflichtete im Zusammenhang mit der Erhebung von Angaben über die Person auch Angaben über das Mittel erheben und speichern müssen, mit dem die Angaben über die Person überprüft wurden. Wenn die verifizierende Organisation die Angaben zur Person mit dem elektronischen Identitätsnachweis gemäß § 12 Abs. 1 S. 1 Nr. 2 GwG (also eID oder Smart-eID) überprüft, hat sie gemäß § 8 Abs. 2 S. 6 GwG iVm § 12 Abs. 1 S. 1 Nr. 2 GwG diese Daten zu erheben und zu speichern: (1) das dienste- und kartenspezifische Kennzeichen; (2) die Tatsache, dass die Prüfung anhand eines elektronischen Identitätsnachweises erfolgt ist.

Nach § 18 Abs. 3 S. 1 PAuswG sind zudem das Sperrmerkmal und die Angabe, ob der elektronische Identitätsnachweis gültig ist, immer zu erheben und zu speichern.

8. Keine „Wiederverwertung" eines Identifizierungsdatensatzes

a) Übertragbarkeit auf SSI

Abschließend ist zu klären, unter welchen Voraussetzungen die Verwendung von SSI-Identitäten als „Wiederverwertung" von Identifizierungsdatensätzen in Betracht kommt. Das ist nur sehr eingeschränkt möglich und widerspräche dem Grundsatz der SSI-Idee, die Datensouveränität der haltenden Personen zu stärken:

§ 17 Abs. 3a GwG erlaubt die Wiederverwertung der Informationen, die ein Dritter im Rahmen einer Identifizierung nach dem GwG erhoben hat. Auf den ersten Blick erscheint es naheliegend, die Nutzung eines Identitätsmerkmals im SSI-Netzwerk als Wiederverwertung im Sinne von § 17 Abs. 3a GwG zu bewerten. Das gilt umso mehr, als in dem Netzwerk diverse ausstellende Organisationen auftreten. Als ausstellende Organisation eines „staatlichen" Identitätsnachweises kommt va die Bundesdruckerei in Betracht. Sonstige Identitätsdatensätze können aber auch von anderen Organisationen ausgestellt werden. So käme auch in Betracht, dass ein Kreditinstitut seine hier sog. „Bank-ID" als ausstellende Organisation einer haltenden Person ausstellt, damit diese sie weiterverwenden kann.

b) Enge Grenzen

§ 17 Abs. 3a GwG ermöglicht nach der Idee des Gesetzgebers „eine sinnvolle Vermeidung wiederholten Identifizierungsaufwands".[65] Allerdings stehen die engen Grenzen des GwG für die Wiederverwertung von Identitätsdatensätzen der Wiederverwertung „staatlicher" Identitäten entgegen. Der „Dritte" kann nämlich nicht jede beliebige Organisation sein. Aus dem Verweis von § 17 Abs. 3a GwG auf § 17 Abs. 1 bis 3 GwG ergibt sich, dass damit va andere Verpflichtete gemeint sind. Nach § 17 Abs. 3 GwG muss die Identifizierung nach den Vorgaben „für die Durchführung der Sorgfaltspflichten von § 10" GwG durchgeführt worden sein. Außerdem muss der Dritte den Identifizierungsdatensatz zur „Begründung einer eigenen Geschäftsbeziehung" erhoben haben.[66]

Auch wenn die Liste der möglichen ausstellenden Organisationen in einer SSI-Infrastruktur lang ist: Der ganz überwiegende Teil der Organisationen, die Identitätsprüfungen durchführen, sind nicht Verpflichtete des GwG. Als Handelsunternehmen, Mobilitätsanbieter, Telekommunikationsunternehmen oder Elektronikhersteller erfüllen sie typischerweise auch nicht dessen Anforderungen an die Identifizierung nach § 10 GwG. Auch staatliche ausstellende Organisationen wie die Bundesdruckerei scheiden aus. Denn sie erstellen Identitätsdatensätze nicht zur Begründung von Geschäftsbeziehungen.

Damit bliebe zwar grundsätzlich Raum für die „Wiederverwertung" von hier sog. „Bank-IDs". Das würde aber zugleich zu einem Konflikt zwischen den Vorgaben des GwG und der Datensouveränität der haltenden Person in SSI-Netzwerken führen. Bei der Wiederverwertung von Identifizierungsdatensätzen, die (andere) Kreditinstitute erhoben haben, kann der dezentrale Aufbau einer SSI-Infrastruktur das Verfahren nicht einhalten, das das GwG für die Wiederverwertung vorsieht. § 17 Abs. 3a, 3 GwG sieht vor, dass der „Zweitverpflichtete" den Identifizierungsdatensatz direkt vom „Erstverpflichteten" erhält. Im SSI-Netzwerk erhielte er ihn aber von der haltenden Person.

IV. Ergebnisse

1. Die Identifizierung einer Person anhand von eID, Smart-eID, Basis-ID oder sonstiger ID-Alternativen ist in SSI-Netzwerken nicht bereits als sog. Wiederverwertung von Identitätsdatensätzen im Sinne von § 17 Abs. 3a GwG zulässig. Die Wiederverwertung nach § 17 Abs. 3a GwG setzt voraus, dass der Dritte, der der geldwäscherechtlich verpflichteten

Organisation den Identitätsdatensatz zur Verfügung stellt, die Identifizierung der Person zur „Begründung einer eigenen Geschäftsbeziehung" durchgeführt hat. Das trifft im SSI-Konzept weder auf die haltende Person, noch auf die die eID, die Smart-eID oder die Basis-ID ausstellende Organisation, noch auf die lizenzgebende Organisation zu. Die Weitergabe einer hier sog. „Bank-ID" von einem Institut an das andere wäre zwar geldwäscherechtlich möglich. Sie widerspräche aber der SSI-Grundidee, dass die haltende Person ihre Daten verwaltet und weitergibt.

2.Dass bei der Identifizierung einer Person mittels SSI-Identitätsnachweisen die im GwG getrennt geregelten Teilakte „Erhebung" und „Überprüfung" von Angaben zusammenfallen, steht der Nutzung von SSI nicht entgegen. Der Gesetzgeber zeigt in § 17 Abs. 3a GwG (Wiederverwertung von Identitätsdatensätzen Dritter), dass er das Zusammenfallen kennt und akzeptiert.

3.Die Identifizierung der haltenden Person kann zum Zeitpunkt der Veröffentlichung dieses Beitrags GwG-konform mit der eID und der Smart-eID durchgeführt werden. Dabei handelt es sich um Nachweise, die nach § 12 Abs. 1 S. 1 Nr. 2 GwG iVm § 18 PAuswG zulässig sind. Die Bindung der eID an die Ausweiskarte widerspricht aber SSI-Prinzipien. Den Befürwortern des Einsatzes der Smart-eID, die auf ein Secure Element zurückgreift, wird

von Marktteilnehmern entgegengehalten, dass die hohen Sicherheitsanforderungen zulasten der Nutzungsfreundlichkeit gehen und viele Nutzende ausschließen, weil Geräte mit der erforderlichen Hardware sehr teuer sind. Ob eine Variante der Smart-eID, die keinen Zugriff auf das Secure Element benötigt, auf § 18 PAuswG gestützt werden kann, ist derzeit offen. Viele Marktteilnehmer bevorzugen die sog. Basis-ID.

4.Bei der Basis-ID handelt es sich nach der Auffassung des BSI wohl derzeit nicht um einen Nachweis, der nach § 12 Abs. 1 S. 1 Nr. 2 GwG iVm § 18 PAuswG zur Überprüfung von erhobenen Angaben über die zu identifizierende Person benutzt werden kann. In Betracht kommt die Entsprechung mit den Anforderungen von § 18 PAuswG aber, sobald die Zertifizierung der verifizierenden Organisation sichergestellt ist (§ 18 Abs. 4 PAuswG) und die Speicherung in einer SSI-Wallet App den Sicherheitsanforderungen an die Speicherung auf dem Smartphone genügt.

5.Die Gründe, die das BSI gegen die hinreichende Sicherheit von SSI-Infrastrukturen mit DLT-Bezug aufzählt, treffen auf die Infrastruktur zu, in der die Basis-ID im Projekt „Digitale Identitäten" zum Zeitpunkt der Abgabe dieses Beitrags genutzt wird. Die Freigabe des BSI, die die zentrale Voraussetzung der Nutzung eines Identitätsmerkmals auf der Grundlage der Experimentierklausel darstellt, erscheint daher zum Zeitpunkt der Veröffentlichung dieses Beitrags *noch nicht* möglich. Möglich erscheint, dass die Nutzung einer weiterentwickelten Variante der Smart-eID, die ohne DLT auskommt, aber wegen des Verzichts auf das Secure Element nach veröffentlichten Standpunkten des BSI möglicherweise *nicht mehr* den Anforderungen von § 18 PAuswG entspricht, auf die Experimentierklausel gestützt werden kann.

6.Da sich das „notwendige Sicherheitsniveau", das das BSI für die Nutzung eines Verfahrens auf Grund der Experimentierklausel feststellen soll, auf die „Erprobung" bezieht, können die an der Erprobung beteiligten Organisationen durch eine „Beschränkung" der Erprobung auch das notwendige Sicherheitsniveau absenken. Die Äußerungen des BSI bedingen damit „als

Reflex" eine „exekutiv indizierte" Sandbox-Nutzung der Basis-ID und alternativer ID-Varianten.

7.Die Nutzung eines SSI-Identitätsnachweises „Basis-ID" und alternativer ID-Varianten als sonstiges gleichwertiges Verfahren zur Überprüfung von Angaben gemäß § 13 Abs. 1 Nr. 2 GwG ist nicht durch die Experimentierklausel gesperrt. Der Wortlaut sowie der Sinn und Zweck von § 13 GwG lassen die Nutzung eines neuen Identifizierungsverfahrens auch zu, ohne dass das Verfahren zuvor in einer Verordnung von BMF und BMI festgelegt und nach Feststellung des notwendigen Sicherheitsniveaus durch das BSI von der BaFin zugelassen wird.

8.Ob die „Basis-ID" oder eine sonstige ID-Alternative zur Erhebung und Überprüfung der Angaben der Person als sonstiges gleichwertiges Verfahren gemäß § 13 Abs. 1 Nr. 2 GwG verwendet werden kann, hängt davon ab, ob die Sicherheit der Nutzung mit der Augenscheinnahme gleichwertig ist. Das hängt von der technischen Entwicklung ab und ggf. davon, ob verifizierende Organisationen das Verfahren ohne Feststellung der Sicherheit durch das BSI auf eigenes Risiko einsetzen wollen. Sobald das Verfahren den Anforderungen von § 18 PAuswG genügt, wäre es aber bereits nach § 12 Abs. 1 S. 1 Nr. 2 GwG als hinreichend sicheres Mittel einzustufen.

9.Verpflichtete, die die eID oder die Smart-eID akzeptieren, müssen zusätzlich das dienste- und kartenspezifische Kennzeichen, die Tatsache, dass die Prüfung anhand dieser IDs durchgeführt wurde, ein Sperrmerkmal und eine Gültigkeitsangabe erheben. Diese Informationen müsste ein für SSI-Netzwerke hergestellter Identitätsnachweis, der auf diesen Verfahren beruht, ebenfalls enthalten.

---

* Der Autor ist Rechtsanwalt/Syndikusrechtsanwalt in einem kreditwirtschaftlichen Spitzenverband.

1 Begriff: Art. 3 Abs. 1 Digital Markets Act (Entwurf COM/2020/842 final v. 15.12.2020).

2 Vgl. Report „Blockchain and Digital Identity" des Blockchain Observatory and Forum der EU-Kommission v. 2. Mai 2019, S. 12 ff.; Überblick: ROFIEG, 30 Recommendations on Regulation, Innovation and Finance, Final Report to the European Commission, Dezember 2019, S. 77 – Der Autor war Mitglied der Expertengruppe ROFIEG.

3 Vgl. Kudra DuD 2022, 22 (23).

4 https://beck-link.de/68d3z (zuletzt abgerufen am 11.1.2022).

5 https://beck-link.de/sc385 (zuletzt abgerufen am 11.1.2022).

6 Siehe: https://beck-link.de/znh55 (zuletzt abgerufen am 11.1.2022).

7 Vgl. BSI, Eckpunktepapier für Self-sovereign Identities (SSI) unter besonderer Berücksichtigung von Distributed-Ledger-Technologie (DLT) v. 8. Dezember 2021, S. 3.

8 Siehe auch: https://beck-link.de/c8ar6 (zuletzt abgerufen am 11.1.2022).

9 https://beck-link.de/d4x6k (zuletzt abgerufen am 11.1.2022).

10 Siehe nur: Atzler/Stiens, Handelsblatt v. 23.12.2021, https://beck-link.de/veds5 (zuletzt abgerufen am 11.1.2022).

11 Siehe nur: Atzler/Stiens, Handelsblatt v. 23.12.2021, https://beck-link.de/veds5 (zuletzt abgerufen am 11.1.2022).

12 Siehe unten III.3.b) und c).

13 BT-Drs. 19/30443, 66.

14 Atzler/Stiens, Handelsblatt v. 23.12.2021, https://beck-link.de/veds5 (zuletzt abgerufen am 11.1.2022).

15 BT-Drs. 19/28164, 47.

16 Ausnahme: für GwG-Zwecke ohnehin irrelevante Self-Attested Attributes, so II.1.a).

17 Siehe unten III.8.

18 Vgl. Atzler/Stiens, Handelsblatt v. 23.12.2021, https://beck-link.de/veds5 (zuletzt abgerufen am 11.1.2022).

19 Vgl. Atzler/Stiens, Handelsblatt v. 23.12.2021, https://beck-link.de/veds5 (zuletzt abgerufen am 11.1.2022); vgl. Schaarschmidt/Schallbruch/Schuck DuD 2022, 12 (13).

20 https://beck-link.de/t8tn8 (zuletzt abgerufen am 11.1.2022).

21 Atzler/Stiens, Handelsblatt v. 23.12.2021, https://beck-link.de/veds5 (zuletzt abgerufen am 11.1.2022).

22 https://beck-link.de/pa82f (zuletzt abgerufen am 11.1.2022); Atzler/Stiens, Handelsblatt v. 23.12.2021, https://beck-link.de/veds5 (zuletzt abgerufen am 11.1.2022).

23 https://beck-link.de/pa82f (zuletzt abgerufen am 11.1.2022).

24 iOS: Secure Enclave; Android: Strongbox.

25 Alternativ kommt zudem die Geltendmachung eines Anspruchs auf Zugang zum Secure Element nach Art. 6 Abs. 1 lit. f DMA-E in Betracht.

26 Atzler/Stiens, Handelsblatt v. 23.12.2021, https://beck-link.de/veds5 (zuletzt abgerufen am 11.1.2022); https://beck-link.de/8yky5 (zuletzt abgerufen am 11.1.2022).

27 Siehe auch: Stellungnahme des BSI v. 11.5.2021 aus einer IFG-Anfrage, https://beck-link.de/ydxk6 (zuletzt abgerufen am 11.1.2022); Kritik: Aretz DuD 2022, 40 (41 f.); Verteidigung: Kudra DuD 2022, 22 (25).

28 Führerschein: https://beck-link.de/n43br; Hotel-Check-In: https://beck-link.de/677na (zuletzt abgerufen am 11.1.2022).

29 Stellungnahme des BSI v. 11.5.2021 aus einer IFG-Anfrage, https://beck-link.de/ydxk6 (zuletzt abgerufen am 30.12.2021).

30 https://beck-link.de/pfvr2 (zuletzt abgerufen am 11.1.2022).

31 BSI, Handlungsleitfaden zur Integration der Smart-eID in ein Nutzerkonto, Entwurf, Version 0.7, 2021.

32 Siehe oben III.3.b).

33 BT-Drs. 19/28169, 21 f. zu § 10a PAuswG als Grundnorm und S. 23 zu § 18 PAuswG.

34 Bspw.: https://beck-link.de/pa82f (zuletzt abgerufen am 11.1.2022).

35 Siehe zuvor: III.3.c)bb); https://beck-link.de/pa82f (zuletzt abgerufen am 11.1.2022).

36 Bspw.: https://beck-link.de/pa82f (zuletzt abgerufen am 11.1.2022).

37 Etwa: https://beck-link.de/d5n5f (zuletzt abgerufen am 11.1.2022).

38 Atzler/Stiens, Handelsblatt v. 23.12.2021, https://beck-link.de/veds5 (zuletzt abgerufen am 11.1.2022).

39 Atzler/Stiens, Handelsblatt v. 23.12.2021, https://beck-link.de/veds5 (zuletzt abgerufen am 11.1.2022).

40 BT-Drs. 18/11555, 119.

41 BaFin AuA GwG 2021, S. 38 f.

42 BeckOK GwG/Frey, 7. Ed. 1.9.2021, GwG § 13 Rn. 1.

43 Näher sogleich unter III.4.b)aa).

44 Siehe oben III.3.c)aa) und bb).

45 Siehe oben III.1.

46 BT-Drs. 19/30443.

47 Gesetz v. 25.6.2021 BGBl. 2021 I 2083 (Nr. 37).

48 Stellungnahme des BSI v. 11.5.2021 aus einer IFG-Anfrage, https://beck-link.de/ydxk6 (zuletzt abgerufen am 11.1.2022) – betraf den Anwendungsfall Hotel-Check-In.

49 Gesetz v. 5.7.2021 BGBl. I S. 2281, 3678 (Nr. 40).

50 Siehe oben III.3.c)bb).

51 „Eckpunktepapier für Self-sovereign Identities (SSI) unter besonderer Berücksichtigung von Distributed-Ledger-Technologie (DLT)" v. 8. Dezember 2021.

52 Stellungnahme des BSI v. 11.5.2021 aus einer IFG-Anfrage, https://beck-link.de/ydxk6 (zuletzt abgerufen am 11.1.2022).

53 „Eckpunktepapier für Self-sovereign Identities (SSI) unter besonderer Berücksichtigung von Distributed-Ledger-Technologie (DLT)" v. 8. Dezember 2021.

54 Siehe oben III.3.c)cc).

55 Stellungnahme des BSI v. 11.5.2021 aus einer IFG-Anfrage, https://beck-link.de/ydxk6 (zuletzt abgerufen am 11.1.2022).

56 BT-Drs. 19/30443, 66.

57 BT-Drs. 19/30443, 66.

58 BaFin AuA GwG 2021, S. 39.

59 BeckOK GwG/Frey, 7. Ed. 1.9.2021, GwG § 13 Rn. 7–9.1.

60 BeckOK GwG/Frey, 7. Ed. 1.9.2021, GwG § 13 Rn. 7–9.1.

61 BT-Drs. 18/11555, 119.

62 BeckOK GwG/Frey, 7. Ed. 1.9.2021, GwG § 13 Rn. 9.

63 BT-Drs. 19/30443, 67.

64 Siehe oben: III.4.b)aa).

65 BT-Drs. 19/13827, 85.

66 Zu weiteren Einschränkungen: BeckOK GwG/Brian, 7. Ed. 1.9.2021, GwG § 17 Rn. 69-75.