E-ID und Identifizierung in der virtuellen Welt

cnlab security AG, Peter Heinzmann, Zuzana Trubini

Version	Beschreibung	Datum
3.0	Schlussversion	02.02.2021

cnlab security AG Obere Bahnhofstrasse 32b CH-8640 Rapperswil-Jona www.cnlab.ch +41 55 214 33 40

Identifizierung in der virtuellen Welt

In der Schweiz soll neu ein elektronisches System für die Ausstellung, Verwaltung und Anwendung der elektronischen Identifizierungsmittel (E-ID) durch Identitätsdienstleister (IdP) betrieben werden.

In diesem Bericht wird aufgezeigt, was genau unter Identifizierung zu verstehen ist, welche Art von Identifizierung man wo braucht und was die vorgeschlagene E-ID für die Bürger bedeutet.

Kurzzusammenfassung

In der virtuellen Welt geschieht Identifizierung in der Regel anhand weniger, meist selbst deklarierter Attribute. Beim E-Government hingegen, ist die staatliche (zivile) Identität gefordert. In der realen Welt wird die staatliche (zivile) Identität durch den Staat sichergestellt. Gemäss dem neuen Bundesgesetz über elektronische Identifizierungsdienste (E-ID-Gesetz, BGEID) soll die staatliche (zivile) Identität beim E-Government und allgemein in der virtuellen Welt im Auftrag des Staats durch private Identitätsdienstleister (IdP) sichergestellt werden. Diese IdP kennen nicht nur die Bewegungsprofile der Kunden im Internet, sie könnten theoretisch auch Identitätsdiebstahl begehen. Den IdP muss daher absolut vertraut werden können. Die Überprüfung der Sicherheit von IdP muss alle Elemente und Verfahren von der Registrierung über die Authentisierung bis hin zu organisatorischen und rechtlichen Fragen wie Verfügbarkeit, Aufsicht, Haftung und Maturität umfassen. Der Staat will mit Hilfe der E-ID seine E-Government Geschäfte abwickeln, was durchaus Sinn macht. Ob die E-ID auch in grossem Stil für die allgemeine Identifizierung in der virtuellen Welt genutzt werden wird, ist fraglich. Einerseits müssten dazu die Internetdienstleister den neuen Schweizer IdP akzeptieren. Andererseits müssten die Personen, die heute IdP wie Google, Facebook oder Twitter nutzen, auf den Schweizer IdP umsteigen. Ferner sind für die Identifizierung in der virtuellen Welt sogenannte Passwort-Manager Lösungen eine durchaus interessante Alternative, vor allem hinsichtlich Datenschutz- und Sicherheitsfragen.

1_ Identifizierung

Unter Identifizierung versteht man einen Vorgang, der zum eindeutigen Erkennen von "Objekten" dient. "Objekte" können Personen, Geräte, Systeme, Anwendungen oder Gegenstände sein. In diesem Bericht geht es um die Erkennung von Personen. Die Identifizierung – man spricht auch von Identifikation, Identitätsfeststellung oder Verifikation - erfolgt anhand kennzeichnender Attribute (Eigenschaften, Merkmale) eines Objekts[1]. Zwei Personen gelten als identisch, wenn sich zwischen ihnen kein Unterschied bezüglich der kennzeichnenden Attribute finden lässt.

In manchen Situationen wird zwischen Identifizierung und Verifizierung (Verifikation) unterschieden:

- Bei der Identifizierung vergleicht man die Attribute einer Person mit den Attributen einer Menge von Referenzdatensätzen und sucht den am besten passenden Referenzdatensatz heraus. Dies ist beispielsweise bei der Bestimmung einer Person anhand von Bildern einer Überwachungskamera der Fall.
- Bei der Verifikation werden dagegen die Attribute einer Person nur mit denjenigen eines einzigen vorgegebenen Referenzdatensatzes verglichen. Dies ist beispielsweise bei einer Personenüberprüfung durch die Polizei oder am Zoll der Fall. Die Verifikation ist somit ein Spezialfall der Identifikation, bei welchem es nur einen Referenzdatensatz gibt, mit welchem die Attribute der Person verglichen werden müssen.

2_ Attribute, Identität und Anonymität

Als Person haben wir eine Vielzahl von Attributen verschiedenster Art (vgl. Figur 1). Manche wurden uns vom Staat zugewiesen, andere von Firmen, manche haben wir selbst gewählt und andere haben sich einfach so ergeben. Biometrische Attribute sind eng mit unserem Körper verbunden, mache davon können wir gar nicht ändern.

[1] Kennzeichnende Attribute bei Objekten sind beispielsweise Unterschriften, Initialen oder Farbarten bei Gemälden und Wasserzeichen bei Dokumenten oder Stempel bei Gegenständen.

Figur 1 Beispiele zur Vielzahl von Attributen einer Person

Abhängig vom Kontext können wir unterschiedliche Identitäten (charakterisiert durch eine Teilmenge der Attribute) annehmen.

In der **realen Welt** sind dies beispielsweise folgende Identitäten:

- Die **staatliche (zivile) Identität** ist, durch die bei der Geburt in den staatlichen Personenregistern erfassten Attribute bestimmt. Darauf basierend werden die hoheitlichen Dokumente (der Pass oder die Identitätskarte) mit den Attributen Gesichtsbild, Name, Vorname(n), Nationalität, Geburtsdatum, Geschlecht und Heimatort erstellt. Die staatliche (zivile) Identität ist beim Verkehr mit Behörden zu verwenden.
- Die **Identität im beruflichen Umfeld** ist durch weitere Attribute bestimmt (z.B. Stellung in der Organisation, Fachkenntnisse oder spezielle Fähigkeiten, Zivilstand).
- Die **Identität im privaten Umfeld** ist bestimmt durch wieder andere Attribute (z.B. Funktion im Sport- oder Musikverein).

Die **Identität einer Person in der virtuellen Welt (digitale Identität)** beruht meistens auf Attributen, welche sich die Person selbst gegeben hat. Dadurch haben Personen in der virtuellen Welt zahlreiche digitale Identitäten, wobei in den meisten Fällen keine rechtsgültige, staatliche Identifizierung möglich ist. Beispiele typischer digitaler Identitäten von Personen sind:

- E-Mail-Adressen im Geschäft und im Privatbereich
- Social Media Benutzername (z.B. Facebook, WhatsApp)
- Benutzernamen auf Computern, Web-Plattformen (z.B. Shops, News-Dienste), Cloud-Diensteanbietern (z.B. Dropbox, Microsoft 365, Google) und Apps (z.B. Fitness Apps)

Schliesslich gibt es sowohl in der realen als auch in der virtuellen Welt Situationen, in denen **Anonymität einer Person** gewünscht wird. Personen wollen nicht erkannt werden, d.h. man soll keinen Bezug zu Identitäten der Person (in der realen oder virtuellen Welt) machen können.

3_ Arten der Identifizierung

Bei Interaktionen mit "Stellen" wie Produkteanbietern (Geschäfte, Shops), Dienstleistern und Behörden wollen diese Stellen sicher sein, dass sie es mit der "richtigen Person" zu tun haben. Als Person will man auch sicher sein, dass man mit der "richtigen Stelle" oder bei der Kommunikation mit der "richtigen anderen Person" zu tun hat. "Richtig" heisst in diesem Zusammenhang, dass die Person oder die Stelle bestimmte kennzeichnende Attribute besitzt.

Tabelle 1 zeigt, welche Attribute bei verschiedenen Geschäftsprozessen bei der Identifizierung einer Person gegenüber der "Stelle" (z.B. einem Geschäft) wichtig sind und anhand welcher Referenz diese überprüft werden.

Geschäftsprozess	**Wichtige, benötigte Attribute**	**Referenz zur Überprüfung der Attribute**	**Ist eine vollständige staatliche Identität erforderlich?**
Identifikation bei Polizeikontrollen, Zoll, Fluggesellschaft	staatliche (zivile) Identität	hoheitliches Dokument	Ja
Einholen eines Strafregisterauszugs			
Standesamtliche Trauung			
Aufnahme von Geschäftsbeziehungen mit einer Bank (Kontoeröffnung, (Know Your Customer Prozess)			
Registrierung eines qualifizierten digitalen Zertifikats			
Datenschutz Auskunftsbegehren			
Volksabstimmung (in der Schweiz)	Per Post erhaltener Stimmausweis	Keine	Nein
Kaufen von Alkohol und Tabak	Mindestalter	hoheitliches Dokument	Nein
Vergünstigung beim Kauf von Dienstleistungen oder Produkten für Pensionierte			
Vergünstigung beim Kauf von Dienstleistungen oder Produkten für Studierende	Studierendenstatus	Studentenkarte einer Universität	Nein
Kauf von Produkten und Dienstleistungen (e-Shopping)	Lieferadresse / E-Mail-Adresse Zahlungsdaten	Reaktion auf E-Mail	Nein
		Evtl. Zahlungsfähigkeit	
Registrierung einer E-Mail-Adresse	keine	Selbstdeklaration	Nein
Registrierung bei einem Web-Portal (z.B. News, Zeitung, Cloud-Services)	E-Mail-Adresse	Selbstdeklaration	Nein

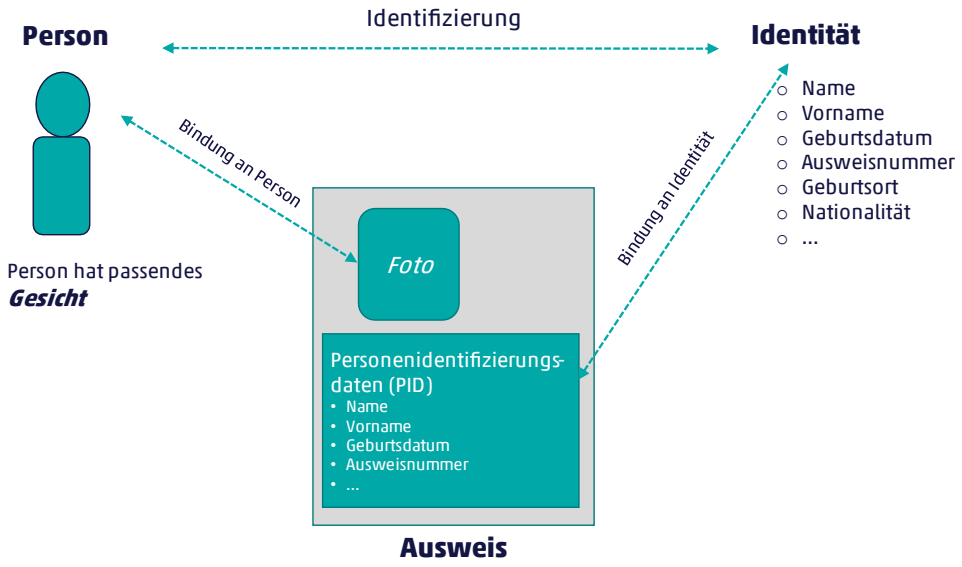
Tabelle 1 Geschäftsprozesse, benötigte Attribute und deren Überprüfung, staatliche Identität

Eine **Identitätsfeststellung**, d.h. eine **Identifikation unter der staatlichen (zivilen) Identität** mit Attributen aus einem hoheitlichen Dokument (Identitätskarte, Pass, Ausländerausweis) ist bei den wenigsten Geschäftsprozessen, nämlich nur bei Geschäften mit Behörden, Finanzinstituten und Versicherungen erforderlich.

3.1 Physische Identifizierung

In der realen Welt erscheint die zu identifizierende Person persönlich bei der Geschäftsstelle und legt entsprechend ausgebildetem Personal den offiziellen Ausweis vor. Man spricht auch von **physischer Identifizierung**.

Der Ausweis ist eine amtliche Urkunde, die eine Bindung zwischen der biologischen Person (bzw. ihrem Foto) und ihrer staatlichen Identität bescheinigt.



Figur 2 Ausweis als Bindeglied zwischen einer Person (mit einem Gesicht) und einer Identität

Um sicherzustellen, dass die zu identifizierende Person eine rechtmässige Besitzerin des Ausweises ist (und folglich auch Trägerin der dort aufgeführten Identitätsattribute), muss das Gesicht der Person mit dem Foto auf dem Ausweis verglichen werden. Im Idealfall wird auch überprüft, ob der Ausweis echt ist, wobei diese Überprüfung unterschiedlich genau erfolgt.

Hat eine Person keinen Ausweis dabei (z.B. bei einer Polizeikontrolle oder bei telefonischen Rechnungsauskünften), so erfolgt die Identifizierung anhand der Überprüfung von Wissen, indem die Person Fragen zu Attributen beantwortet, welche auf einer Datenbank mit Geschäfts- oder Ausweisinformationen abgelegt sind (z.B. Angabe von Name, Alter, Heimatort oder kürzlich getätigten Transaktionen).

3.2 Digitale Identifizierung

Will man nun Geschäfte digitalisieren, muss man die physische Identifizierung durch entsprechende digitale Identifizierung ablösen. Die in der Schweiz vorhandenen staatlichen Ausweise sind für die Identifizierung im virtuellen Raum aber leider nicht gerüstet.

Die Eidgenössische Finanzmarktaufsicht FINMA lässt zwar für die Identifikation bei der Aufnahme von Geschäftsbeziehungen mit einer Bank (Kontoeröffnung) auch Videoidentifizierung übers

Internet zu, diese Video-Identifizierungsverfahren bilden aber lediglich das physische Identifizierungsverfahren nach. Dabei muss mit dem Kunden eine Videoverbindung aufgebaut werden und es müssen mindestens drei zufällig ausgewählte optische Sicherheitsmerkmale der staatlichen Identifizierungsdokumente überprüft werden. Dies ist umständlich und nur bedingt sicher.

Da die Identifizierung mit einem physischen Ausweis im Allgemeinen auf einer optischen Gesichts- und Echtheitsprüfung basiert, sind physische Ausweise für digitale Identifizierungen schlecht geeignet und müssen durch neue, elektronische Identifizierungsmittel (E-ID) ersetzt werden.

Das **Bundesgesetz über elektronische Identifizierungsdienste** (E-ID-Gesetz, BGEID) legt die Rahmenbedingungen für die digitale Identifizierung natürlicher Personen für den elektronischen Geschäftsverkehr unter Privaten und mit Behörden fest (Bundesgesetz über elektronische Identifizierungsdienste (E-ID-Gesetz, BGEID), 27. September 2019). Zu diesem Gesetz wurde das fakultative Referendum ergriffen[2]. Beanstandet wird vor allem, dass das Gesetz die Entwicklung und den Vertrieb bzw. die Ausgabe der elektronischen Identifizierungsmittel (E-ID) durch private Identitätsdienstleiser (Identity Provider, IdP) wie die SwissSign Group vorsieht. Mit derselben Rollenteilung hat der Bund vor zehn Jahren die qualifizierte, elektronische Unterschrift eingeführt. Diese hat aber keine breite Verwendung gefunden. Das liegt unter anderem daran, dass die Erstellung einer qualifizierten digitalen Signatur erst nach einer Registrierung und der damit verbundenen physischen[3] Identitätsprüfung durch einen IdP möglich ist.

Die **EU-Verordnung Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt** (electronic IDentification, Authentication and trust Services, eIDAS) regelt EU-weit den Einsatz von Vertrauensdiensten und elektronischer Identifizierung (EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt [eIDAS Verordnung EU Nr. 910/2014], 23. Juli 2014). Die eIDAS-Verordnung ist im kompletten europäischen Wirtschaftsraum und in allen 27 Mitgliedsstaaten der EU unmittelbar geltendes Recht. eIDAS will elektronischen Transaktionen ähnliche rechtliche Stellung verschaffen, wie Transaktionen auf Papier.

[2] Das Referendum zum E-ID-Gesetz kommt voraussichtlich im Frühjahr 2021 zur Abstimmung.

[3] Im Zuge der Corona-Notmassnahmen hat der Bundesrat die Verordnung über die elektronische Signatur (VZertES) [1] am 1. April 2020 für eine befristete Dauer von sechs Monaten angepasst, so dass die Registrierung per Video-Identifikation als Alternative zur physischen Identifizierung möglich ist.

4_ Registrierung

Damit sich eine Person überhaupt identifizieren kann, müssen ihre Identitätsattribute Attribute im Rahmen eines Registrierungsprozesses erfasst, und auf einer Datenbank und/oder einem physischen Dokument abgelegt werden.

Für Schweizer Staatsangehörige besorgt der Staat bzw. die in den Kantonen bezeichneten Stellen die Registrierung für die Ausgabe von Identitätskarte und Pass (Bundesgesetz über die Ausweise für Schweizer Staatsangehörige (Ausweisgesetz, AwG), 22. Juni 2001). Dabei werden Personendaten aus dem elektronischen Personenstandsregister (Infostar) in das Informationssystem Ausweisschriften (ISA) übernommen. Die antragstellende Person muss persönlich bei der ausstellenden Behörde vorsprechen und sich über ihre Identität ausweisen.

Die ausstellende Behörde erstellt im Rahmen des Registrierungsprozesses von der antragstellenden Person eine digitale Fotografie und erfasst zwei Fingerabdrücke (des linken und rechten Zeigefingers). Schweizer Pass und Identitätskarte enthalten die Merkmale Gesichtsbild, Name, Vorname(n), Nationalität, Geburtsdatum, Geschlecht, Heimatort, Ausstellungsbehörde und Gültigkeitsdatum, wobei die Daten beim Pass zusammen mit den Fingerabdruckdaten auch in elektronischer Form auf einem Chip abgespeichert sind.

Auch in der digitalen Welt werden bei der Registrierung Attribute erfasst. Je nach Situation müssen die erfassten Attribute überprüft werden. Wenn die digitale Identität einer Person sicher an ihre staatliche Identität gebunden werden soll (z.B. bei einer Kontoeröffnung), muss diese anhand eines hoheitlichen Dokumentes überprüft werden. In anderen Fällen ist Selbstdeklaration oder allenfalls eine Überprüfung der E-Mail-Adresse ausreichend.

Im Rahmen der Registrierung werden ebenfalls die Authentisierungsmittel des Benutzers festgelegt (z.B. Passwortwahl) und mit seiner digitalen Identität verknüpft.

5_ Authentifizierung

Authentifizierung[4] steht für die Verifizierung der Identität einer Person als Benutzer einer Informatik-Anwendung durch das Informatik-System (Rechner, Server, Programm). Ein Benutzer authentisiert sich, indem er persönliche Attribute[5] vorlegt, welche das System verifizieren bzw. überprüfen kann. Dabei unterscheidet man drei Klassen (Faktoren) von Attributen. Es kann danach gefragt werden

- was jemand weiss (z.B. ein Passwort, ein PIN-Code) - kognitive Identifikation (Wissen)
- was jemand besitzt (z.B. Badge, einen kryptographischen Schlüssel) - possessive Identifikation (Besitz)
- welche biologischen Attribute (Merkmale) jemand hat (z.B. Fingerabdruck, Gesichtsbild, genetischer Fingerabdruck bzw. DNA-Profil) - existentielle bzw. biometrische Identifikation (Sein).

Sind für die Authentifizierung zwei verschiedene Arten von Attributen (z.B. Wissen und Besitz) nötig, so spricht man von Zwei-Faktor-Authentifizierung. Je mehr Attribute bei einer Authentifizierung überprüft werden, desto sicherer ist es, dass es nicht zu Verwechslungen von Personen kommen kann. Falls sich jemand als eine andere Person ausgeben kann, spricht man von Identitätsdiebstahl, Identitätsmissbrauch, Identitätsveränderung oder Identitätswechsel (engl. impersonation).

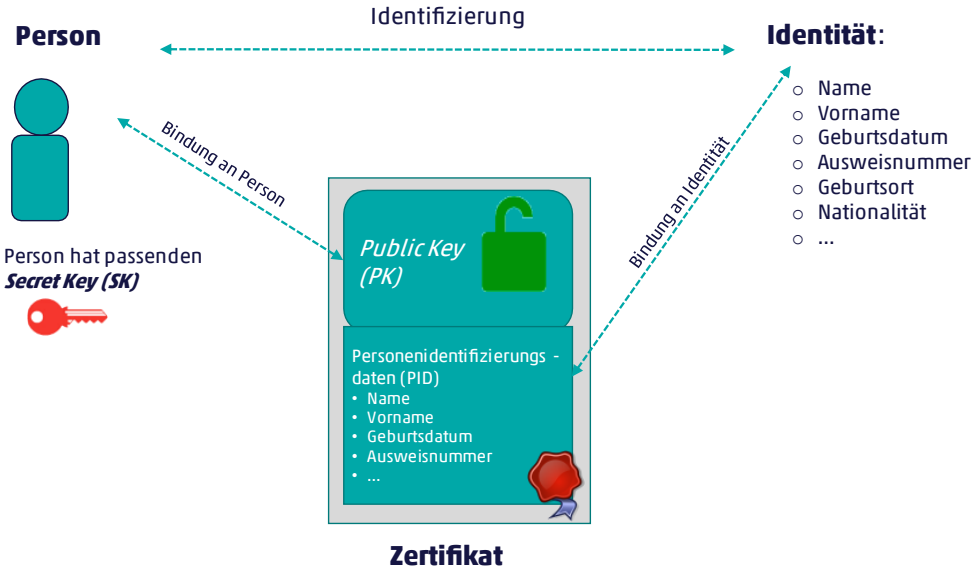
Bei der Authentifizierung werden die Attribute, Verfahren und Prozesse mit kryptographischen Mitteln so gesichert, damit die Identitäten nicht gefälscht oder gestohlen werden können, d.h. dass Identitätsdiebstahl nicht möglich ist.

5.1 Zertifikatsbasierte Authentifizierung

Bei der **zertifikatsbasierten Authentifizierung** wird ein digitales Zertifikat verwendet, um einen Benutzer (ein Gerät oder einen Computer) zu identifizieren. Ein digitales Zertifikat ist ein von einer Zertifizierungsinstitution als echt erklärter und digital unterschriebener öffentlicher Datensatz, der die Identitätsattribute einer Person (bzw. eines Computers) mit deren Public-Key (PK) verbindet. Nur der Eigentümer des Zertifikats besitzt den zum Public-Key zugehörigen geheimen Schlüssel (Secret-Key, SK), mit dessen Hilfe er einem Verifier beweisen kann, dass er der Besitzer des Zertifikats ist. Ein Zertifikat ist also ein digitales Analogon eines Ausweises und kann zur digitalen Identifizierung und Authentisierung genutzt werden.

[4] Im deutschen Sprachraum wird im Gegensatz zum englischen Sprachraum zwischen Authentifizierung (Authentifikation) und Authentisierung unterschieden. Authentifizierung steht für die Prüfung der Echtheit durch den Dienstanbieter und Authentisierung steht für den Beweis ihrer Echtheit durch die Person.

[5] Persönliche Attribute sind im Gegensatz zu den Identitätsattributen private, der Person zugehörige Attribute, die für die Überprüfung der Authentizität verwendet werden können, wie z.B. biometrische Eigenschaften und Geheimnisse.



Figur 3 Zertifikat als Bindeglied zwischen einer Person (einem Secret Key Besitzer) und einer Identität

Der zum Zertifikat passende geheime Schlüssel ist auf einer "Authentifikator App" auf einem Token (Smartphone, USB-Stick oder SmartCard) abgespeichert und kann typischerweise nur nach Eingabe eines Geheimcodes (PIN) oder Vorweisung eines biometrischen Merkmals (Fingerabdruck, Gesicht, Iris) verwendet werden. Somit liegt hier eine Zwei-Faktor-Authentisierung vor mit der Überprüfung von Besitz (USB-Stick, SmartCard) und Wissen (PIN) oder Sein (biometrisches Merkmal).

Die zertifikatsbasierte Authentisierung war früher wegen Hardware und Software (Treiber) Problemen bei unterschiedlichen IT-Systemen aufwändig und mit relativ viel Supportaufwand verbunden. Durch die Weiterentwicklung der Technologien und Standards sind zertifikatsbasierte Authentisierungsverfahren wesentlich einfacher und durchaus praktikabel für den breiten Einsatz geworden, wie die weite Verbreitung zertifikatsbasierter Authentisierung bei verschiedenen eIDAS-Implementierungen (z.B. in Estland, Dänemark) beweist.

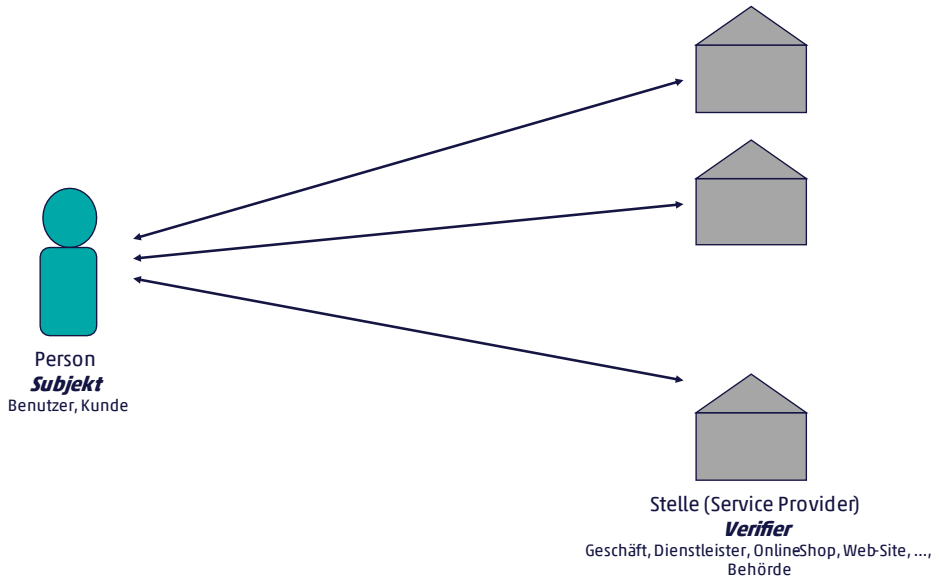
Die Echtheit eines Zertifikats kann anhand der digitalen Signatur der Zertifizierungsinstitution überprüft werden. Der von der Zertifizierungsstelle durchgeführte Registrierungsprozess ist die Basis für eine zuverlässige Identifizierung anhand eines Zertifikats. Für Zertifikate, welche eine qualifizierte, digitale Signatur ermöglichen, muss der Zertifikatsaussteller die staatliche Identität verifizieren, d.h. bei der Registrierung hat die Person die hoheitlichen staatlichen Dokumente (Identitätskarte, Pass) vorzuweisen und die Registrierungsstelle muss diese überprüfen.

In einigen Ländern ist das digitale Zertifikat und der geheime Schlüssel bereits in der staatlichen Identitätskarte enthalten.[6] Damit entfällt die Notwendigkeit einer zusätzlichen Registrierung und der damit verbundener Identitätsprüfung. Die Identitätskarte ist somit direkt als elektronisches Identifizierungs- und Authentisierungsmittel einsetzbar und kann überall dort verwendet werden, wo der Bürger unter seiner staatlichen Identität auftreten muss (oder möchte).

[6] Auf das Zertifikat kann dabei jederzeit zugegriffen werden, der geheime Schlüssel ist hingegen durch eine PIN geschützt.

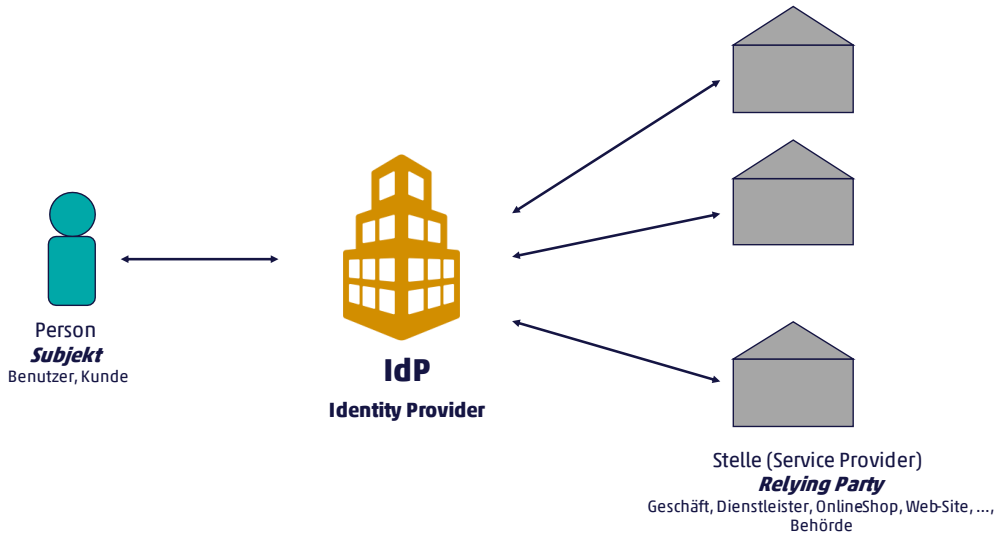
6_ Identifizierungsdienste

In Ländern ohne eine befriedigende E-ID Lösung müssen sich Personen in der virtuellen Welt **bei sehr vielen Stellen separat registrieren und je nach Situation auch eine Identitätsprüfung durchlaufen**. Die Stelle (der Service Provider) übernimmt dabei sowohl die Registrierung als auch die Authentifikation (Verifikation). Die Registrierung ist oft aufwendig und bei der Authentisierung mit Benutzername und Passwort mit so vielen unterschiedlichen Stellen leidet die Sicherheit: Man verliert die Übersicht, wo überall man sich registriert hat und einfachheitshalber verwenden viele Leute gleiche oder sehr einfach zu merkende, unsichere Passwörter.



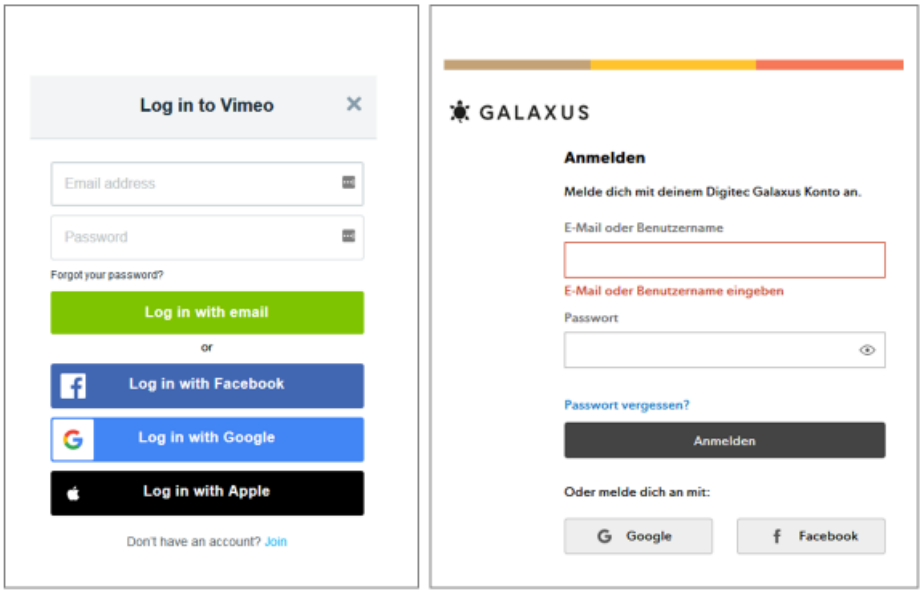
Figur 4 Typische Identifizierung in der virtuellen Welt

In den letzten Jahren sind so genannte **Identifizierungsdienste (Identity Provider, IdP)** eingeführt worden, welche die Identifizierung und Authentifizierung für verschiedenste Stellen – sogenannte Relying Parties (RP) - übernehmen. Dabei registrieren und authentisieren sich die Personen nur noch bei ihrem IdP, der dann ihre Identität gegenüber der Relying Party bezeugt. Man spricht in diesem Zusammenhang auch von Identity-Federation. Viele IdP bieten auch einen sogenannten Single-Sign-On (SSO) Dienst an, was bedeutet, dass sie nach einer einmaligen Authentifizierung eines Benutzers seine Identität (innerhalb einer gewissen Zeit) gegenüber mehreren Stellen bezeugen.



Figur 5 Identifizierung und Authentisierung mit Identity Provider (IdP)

Weil man für die Authentisierung häufig die entsprechenden Social Media Accounts nutzt, spricht man auch von "Social Login". Die bekanntesten, mittlerweile weltweit genutzten IdP sind Google, Facebook, Twitter und Apple (Vapen, Carlsson, Mahanti, & Shahmehri, 26 February 2016). Diese IdP-Lösungen bieten aber keine staatliche Identität an.



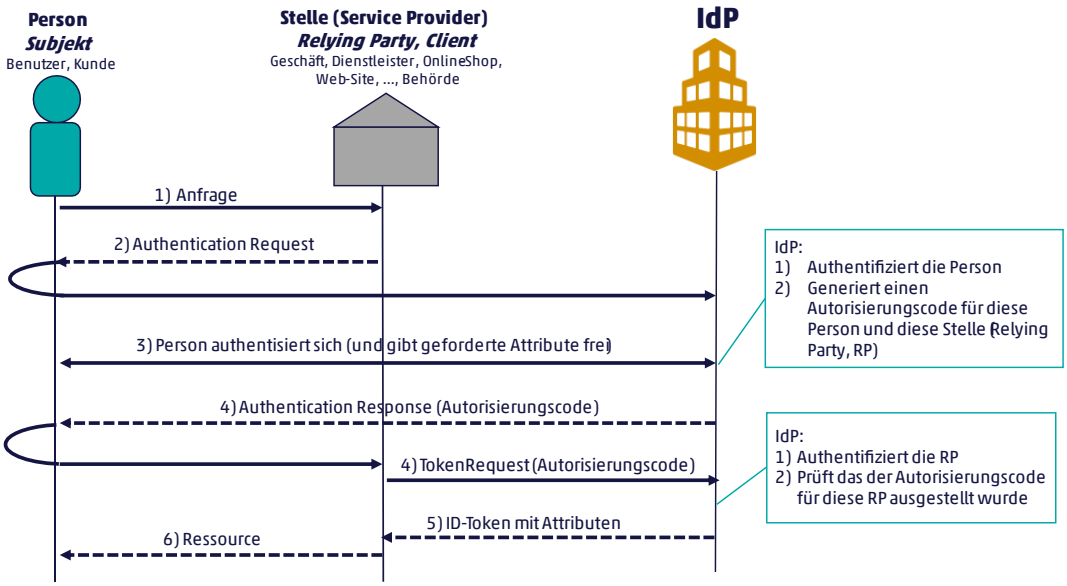
Figur 6 Login über weltweit genutzte IdP (Beispiel zur Videoplattform Vimeo und zum Internetshop Galaxus)

Im Rahmen der Registrierung einer Person beim Identity Provider werden ihre Identitätsattribute erfasst und allenfalls auch geprüft[7]. Es wird auch festgelegt, wie sich die Person in Zukunft beim IdP zu authentisieren hat.

Will sich nun eine Person bei einem Online-Shop unter ihrer Google-Identität (mit ihrem Google-Login) anmelden, wird sie von der Shop-Seite zu Google umgeleitet. Der Online-Shop (als Relying Party) schickt dabei einen sogenannten Authentication-Request an Google, in dem er spezifiziert welche Identitäts-Attribute (z.B. Name, E-Mail-Adresse, Geschlecht) er als Antwort erhalten möchte und allenfalls auch welche Art der Authentisierung verlangt wird. Google (in der Rolle des IdP) authentifiziert die Person, holt von ihr das Einverständnis für die Übergabe ihrer Identitätsattribute an den Online-Shop und leitet die Person zum Online-Shop zurück. Der Online-Shop erhält von Google eine sogenannte Assertion - eine Zusicherung, dass sich der Benutzer korrekt authentisiert hat. Diese Assertion enthält einen Identifikator des Benutzers und ev. weitere Attribute seiner Identität (Name, E-Mail-Adresse, Geschlecht).

Für die Authentisierung via einen IdP wird in der Regel der OpenID Connect Standard (Sakimura, Bradley, Jones, de Medeiros, & Mortimore, 2014) verwendet, der seinerseits auf dem Autorisierungsstandard OAuth 2.0 basiert.

Der grundsätzliche Ablauf der verschiedenen Meldungen zur Identifikation ist in Figur 7 dargestellt[8].



Figur 7 Beispiel des Meldungsablaufs zur Identifikation (gemäss OpenID Connect)

[7] Die Menge der erfassten Identitäts-Attribute und die Art und Weise wie diese überprüft werden definiert die sogenannte Identifizierungsstärke.

[8] Leider sind die Begrifflichkeiten je nach Standard unterschiedlich. Bei OpenID Connect (OIDC) spricht man von OpenID Provider (OP) und Relying Party (RP). Beim Security Assertion Markup Language (SAML) Standard spricht man von Identity Provider (IdP) und Service Provider (SP).

6.1 Sicherheit von Identifizierungsdiensten

Die Sicherheit von Identifizierungsdiensten bei einem Geschäftsprozess (Dienstleistung, Produktverkauf, Transaktion) ist durch die Schwierigkeit bestimmt, eine falsche Identität vorgeben zu können in Bezug auf die Attribute, welche bei der Registrierung festgelegt wurden. Durch die Vorgabe der falschen Identität können Angreifer Systeme oder Dienste nutzen, die einer anderen Person zustehen. Man spricht in diesem Zusammenhang auch von «Identitätsmissbrauch» oder «Identitätsdiebstahl».

Bei der staatlichen, rechtsgültigen Identität in der realen Welt kann sich eine Person als eine andere Person ausgeben, indem sie beispielsweise den Ausweis fälscht oder sich mit einer speziell gefertigten Maske ein Erscheinungsbild entsprechend dem auf dem Ausweis vorhandenen Gesichtsbild erstellt.

Bei den digitalen Identitäten in der virtuellen Welt, also auch bei der staatlichen, rechtsgültigen Identität in der virtuellen Welt, wie sie beispielsweise gemäss E-ID-Gesetz in der Schweiz oder eIDAS im EU-Raum vorgesehen ist, kann sich eine Person als eine andere Person ausgeben, indem sie beispielsweise Überprüfungen bei der Registrierung oder Authentisierung austrickst. Je nach Authentisierungsverfahren fällt das mehr oder weniger schwer. Beruht eine Authentisierung beispielsweise lediglich auf einem Passwort, so muss der Angreifer einfach das Passwort der Person in Erfahrung bringen oder erraten. Typischerweise werden Passworte mit sogenannten Phishing Attacken "ergaunert", bei welchen man die anzugreifende Person mit geschickt formulierten Mails dazu bringt, das Passwort an Fremde weiterzugeben.

Zur Verhinderung von Identitätsmissbrauch muss man nicht nur die eigentliche Authentisierung, sondern alle mit der Identifizierung verbundenen Prozesse (inkl. Registrierung, allfällige Erneuerungen, Passwort Wiederherstellungsprozesse, Zusammenspiel von Relying Party und IdP) sicher gestalten. Das amerikanische National Institute of Standards and Technology (NIST) hat in seinen Richtlinien zur digitalen Identität (Digital Identity Guidelines) (Digital Identity Guidelines, 2017) die verschiedenen Prozesse beschrieben und passende Anforderungen definiert. Das NIST unterscheidet dabei Identifizierungsstärken, Authentisierungsstärken und Sicherheitsstufen der Föderation:

Identifizierungsstärken (Identity Assurance Levels, IAL)

- IAL1: Es muss kein Bezug zu einer in der realen Welt existierenden Identität bestehen. Die erfassten Attribute werden nicht geprüft – sie sind selbstdeklariert.
- IAL2: Überprüfung von Attributen der staatlichen Identität vor Ort oder Remote.
- IAL3: Persönliche Überprüfung von Attributen der staatlichen Identität durch ausgebildetes Personal vor Ort oder in einer überwachten Video-Session.

Authentisierungsstärken (Authenticator Assurance Level, AAL)

- AAL1: Verifikation anhand von einem Faktor
- AAL2: Verifikation anhand von zwei Faktoren

- AAL3: Verifikation anhand von zwei Faktoren mit Hilfe kryptographischer Schlüssel (symmetrisch oder asymmetrisch) die in einem Hardware-Authentifikator gespeichert sind. Das Authentifizierungsverfahren muss zudem Verifier-Impersonation resistent sein.

Stärke der Föderation bzw. des Zusammenspiels von Relying Party (RP), IdP und Person (Federation Assurance Levels, FAL)

- FAL1: Die Zusicherung (Assertion) für die RP muss vom IdP unterschrieben aber nicht verschlüsselt sein.
- FAL2: Die Zusicherung für die RP muss unterschrieben und verschlüsselt sein.
- FAL3: Die Zusicherung für die RP muss unterschrieben und verschlüsselt sein. Sie muss zusätzlich eine Referenz zu einem geheimen Schlüssel enthalten, dessen Besitz der Benutzer der RP beweisen muss (sogenannte "holder of key assertion").

Diese Anforderungen helfen die Benutzer vor Identitätsdiebstahl zu schützen. Es ist aber zu beachten, dass im Falle eines korrupten oder kompromittierten IdP weder Datenschutz noch die Sicherheit der Identifizierung gewährleistet sind.

Ein IdP (oder ein Angreifer, der den IdP unter Kontrolle hat) ist in der Lage, seine Benutzer zu überwachen. Er sieht beispielsweise, mit welchen Geschäften die Personen, welche den IdP nutzen, kommunizieren. Man sagt, dass IdP wie Google, Facebook oder Twitter ihre Dienste gratis anbieten, weil sie damit Nutzungsdaten gewinnen können. Ein korrupter oder kompromittierter IdP kann auch Identitätsdiebstahl begehen oder neue Identitäten kreieren.

Solche Risiken kann man mit organisatorischen Massnahmen reduzieren. Beispielsweise schützt ein 4-Augen-Prinzip bei der E-ID-Erstellung vor korrupten Mitarbeitern. Die getrennte Datenhaltung (Personenidentifizierungsdaten und Nutzerdaten getrennt) schützt vor dem Missbrauch von Personendaten. Ein redundanter Aufbau und Betrieb der IdP-Systeme, stellt die Verfügbarkeit der Services der Relying Parties sicher.

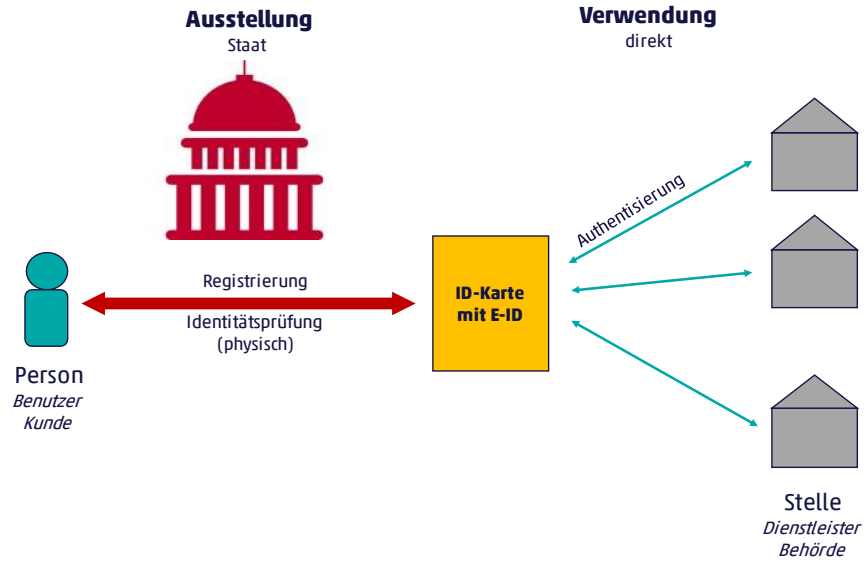
Die Einhaltung der organisatorischen Massnahmen ist gemäss E-ID-Gesetz gesetzlich festgelegt und soll durch akkreditierte Stellen überwacht werden. Bei "Identifizierungsdiensten für Schweizer E-Government Anwendungen" werden zu organisatorischen Massnahmen unter dem Begriff «Steuerung» die Kriterien Aufsicht, Haftung und Maturität aufgeführt (Laube-Rosenpflanzer, Hassenstein, & Kunz, 13.09.2017).

7_ Staatliche Identität in der virtuellen Welt

Immer mehr Länder bieten ihren Bürgern eine staatliche Identität für die virtuelle Welt an. In Europa sind dies beispielsweise Belgien, Deutschland, Estland, Finnland, Italien, Litauen, Luxemburg, Norwegen, Österreich, Portugal, Schweden, Tschechische Republik.

Die Vorreiterrolle auf diesem Gebiet gehört Estland – dort ist die E-ID schon seit über 10 Jahren Teil der ID-Karte. Die Estländische Identitätskarte beinhaltet eine digitale Komponente bestehend aus einem digitalen Zertifikat und einem PIN-geschützten geheimen Schlüssel. Mit dieser können sich alle Bürger unter ihrer staatlichen Identität digital identifizieren und diese im virtuellen Kontakt mit Banken, Behörden, Gesundheitsdiensten usw. verwenden.

Diese Lösung basiert auf weltweiten Standards (X.509 Zertifikat und mutual Authentication Transport Layer Security, mTLS) und bietet die höchste Sicherheit (IAL3, AAL 3). Die Personen können sich mit der (in der ID-Karte enthaltenen) E-ID direkt bei den Stellen authentisieren, deren Dienste sie in Anspruch nehmen wollen (Wikipedia, kein Datum). Dabei kommen sie ohne einen IdP aus, womit auch alle mit der Nutzung von IdP verbundenen Risiken (z.B. Datenschutz) entfallen. Da die E-ID Teil der ID-Karte ist, entfällt weiter die Notwendigkeit der Registrierung und der damit verbundenen aufwendigen Identitätsprüfung.



Figur 8 Ausstellung und Verwendung einer in eine ID-Karte integrierten zertifikatsbasierten E-ID

In der Schweiz gibt es im Moment noch keine staatlich anerkannte E-ID. Seit Ende 2017 besteht für die Identifikation mit einer staatlichen Identität die SwissID IdP-Lösung.

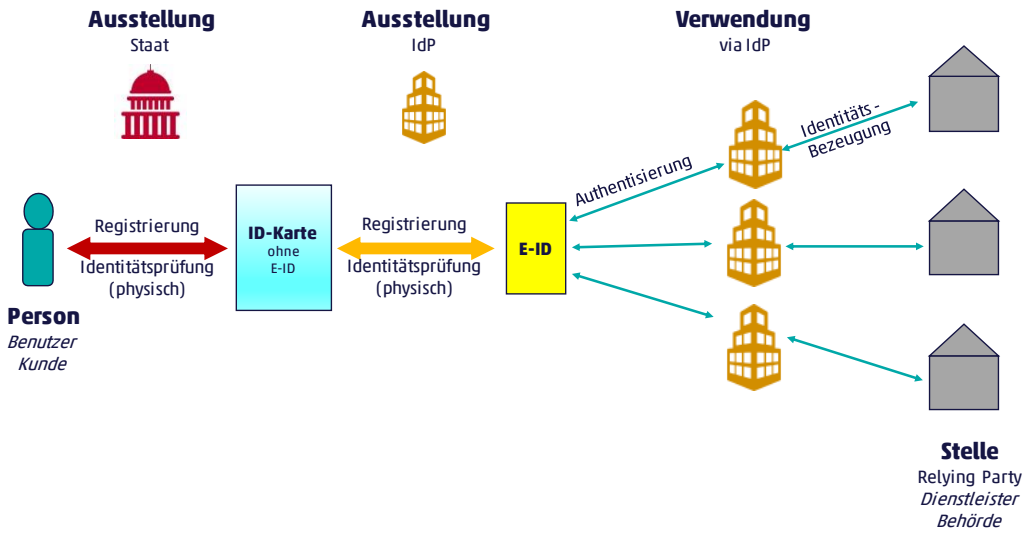
SwissID wird von der SwissSign Group AG angeboten, einem Gemeinschaftsunternehmen von staatsnahen Firmen (Post, SBB, Swisscom), Finanzdienstleistern (UBS, ZKB, SGKB, GEKB, Entris Banking, SIX), Versicherern (AXA, Baloise, Helvetia, Mobiliar, Swiss Life, Vaudoise, Zürich) und Krankenkassen (CSS, Swica). Die SwissSign Group AG ist das Nachfolgeunternehmen der SwissSign AG, welche seit der Gründung 2001 mit verschiedenen Unterstützungspaketen des Bundes

unter der Bezeichnung SuisseID qualifizierte, elektronische Zertifikate auf USB-Stick oder Chipkarte anbot. Die SwissSign AG hat mit einer Finanzierungshilfe des Bundes in der Höhe von 17 Millionen Franken bis Ende 2010 lediglich 270'000 SuisseID herausgegeben, die mehrheitlich nicht mehr erneuert wurden (Hirter, Braun, Langhart, & Gmünder, August 2016). Die Gründe, dass sich die SuisseID bisher nicht im Markt durchsetzen konnte, waren neben der Komplexität der Beschaffung und Nutzung der digitalen ID wohl auch die Kosten (ca. Fr. 80 pro Person und Jahr), die fehlenden Nutzungsmöglichkeiten oder einfach der fehlende Bedarf nach einer digitalen ID.

7.1 Staatliche E-ID gemäss Schweizer E-ID-Gesetz

Das Bundesgesetz über elektronische Identifizierungsdienste regelt den Inhalt, die Ausstellung, Verwendung, Sperrung und Widerruf von staatlich anerkannten elektronischen Einheiten, die zur Identifizierung natürlicher Personen verwendet werden (Bundesgesetz über elektronische Identifizierungsdienste (E-ID-Gesetz, BGEID), 27. September 2019), (Botschaft zum Bundesgesetz über elektronische Identifizierungsdienste, 1. Juni 2018).

Mit einer E-ID sollen sich natürliche Personen sicher und bequem bei E-Government-Diensten registrieren und später wieder anmelden können. Die E-ID wird aber auch für den Einsatz bei allgemeinen Online-Diensten (Internet-Diensten) angepriesen, welche keine vollständige staatliche Identität benötigen. Die vorgesehene E-ID Lösung orientiert sich stark an der SwissID-Lösung, bei der ein IdP sowohl bei der Ausstellung als auch bei der Verwendung der E-ID eine zentrale Rolle spielt (vgl. Figur 9).



Figur 9 Ausstellung und Verwendung der geplanten IdP-basierten Schweizer E-ID

Gemäss dem Gesetz, der Botschaft zum Gesetz und dem E-ID-Konzept soll die E-ID in drei verschiedenen Sicherheitsniveaus erhältlich sein, welche sich in Bezug auf den Prozess der E-ID Ausstellung, die Stärke der E-ID Authentifizierung und die Betriebssicherheit des E-ID-Systems unterscheiden:

- **Ausstellungsprozess:** Stärke der Identitätsprüfung, Menge der vom Bund zum IdP übertragenen Attribute (Personenidentifizierungsdaten, PID)
- **Authentisierungsstärke:** Anzahl und Art der Authentisierungsfaktoren
- **Betrieb des E-ID-Systems:** Häufigkeit der Aktualisierung der Personenidentifizierungsdaten

Die drei Sicherheitsniveaus sind in Tabelle 2 charakterisiert:

Sicherheitsstufe	**Niedrig**	**Substanziell**	**Hoch**
Registrierung			
Identitätsprüfung	Online (z.B. mit einer Ausweiskopie, ohne Gesichts- und Echtheitsprüfung)	Abgleich des Gesichtsbildes des Antragsstellers mit dem Foto auf seinem Ausweis	Persönliche Vorsprache oder online mit Videoidentifikation Überprüfung der Echtheit des Ausweises und mindestens eines biometrischen Merkmals gestützt auf eine behördliche Quelle (z.B. Ausweisgültigkeit und Gesichtsbild)
Attribute	▪ E-ID-Registrierungsnummer ▪ bereits auf dem Ausweis enthaltenen Attribute	▪ E-ID-Registrierungsnummer ▪ Namen, Vornamen ▪ Geburtsdatum ▪ Geschlecht ▪ Geburtsort ▪ Staatsangehörigkeit	▪ E-ID-Registrierungsnummer ▪ Namen, Vornamen ▪ Geburtsdatum ▪ Geschlecht ▪ Geburtsort ▪ Staatsangehörigkeit ▪ Gesichtsbild des Antragstellers aus dem Informationssystem des Bundes
Authentisierung			
Authentisierungsfaktoren	Ein-Faktor (z.B. Passwort)	Zwei-Faktor-Authentisierung (z.B. Passwort und mTAN)	Zwei-Faktor-Authentisierung, wobei ein Faktor biometrisch sein muss (z.B. Fingerabdruckgeschützter Secret Key in einer Smartphone-App)
Zusätzliche Massnahmen	keine	keine	Zusätzlich muss das Authentifizierungsmittel einen direkten Nachweis der Authentifizierung des Inhabers liefern können, der vom E-ID verwendenden Dienst überprüft werden kann.
Betrieb			
Aktualisierung	jährlich	quartalsweise	wöchentlich
Stärke der Föderation bzw. des Zusammenspiels von RP, IdP und Person	E-ID Gesetz beschreibt diesbezüglich keine klaren Anforderungen		

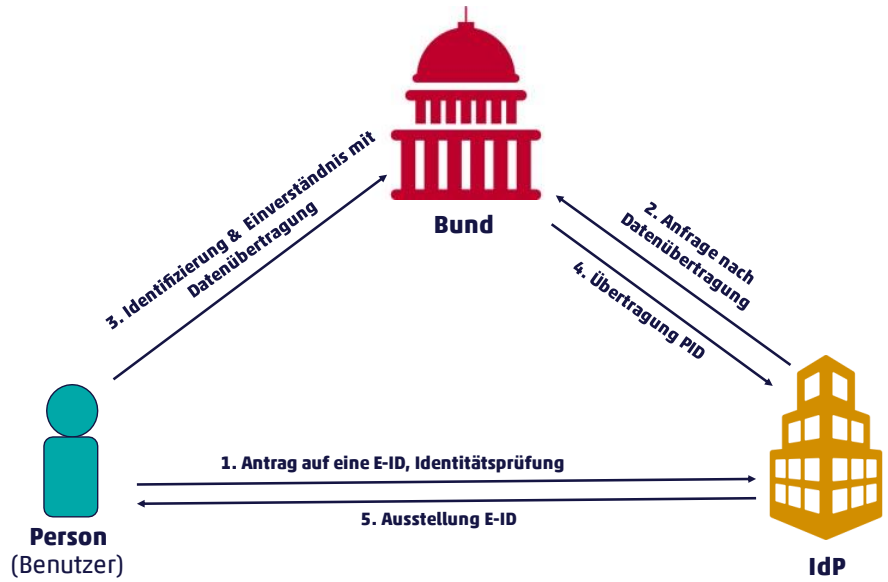
Tabelle 2 Sicherheitsstufen bei der E-ID

Diese Sicherheitsniveaus unterscheiden sich (entgegen der Behauptung in der Botschaft) in gewissen Punkten von den NIST Sicherheitsniveaus - sowohl bezüglich Identifizierungsstärken

(Identity Assurance Levels, IAL) als auch bezüglich Authentisierungsstärken (Authenticator Assurance Level, AAL). Zu Federation Assurance Levels (FAL) werden gar keine Vorgaben gemacht.

Der Ausstellungsprozess der E-ID wird wie folgt ablaufen (vgl. Figur 10):

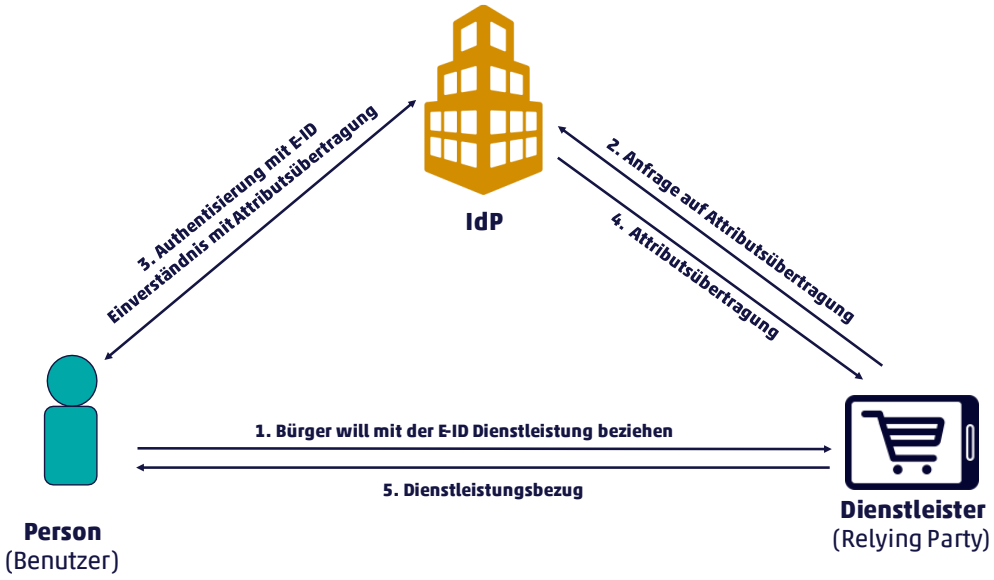
0. Der IdP wird vom Bund geprüft und anerkannt.
1. Eine Person beantragt die Ausstellung der E-ID bei einem IdP ihrer Wahl. Dieser führt die initiale Identitätsprüfung durch (je nach Sicherheitsniveau).
2. Der IdP leitet dann die Daten zur Person an den Bund weiter.
3. Der Bund identifiziert die Person mit Hilfe ihrer Identitätsattribute, authentifiziert sie anhand zusätzlicher Fragen zu persönlichen Daten (Information über Eltern oder über andere Ausweisdokumente) und holt ihr Einverständnis für die Datenübertragung ein.
4. Der Bund übermittelt die dem Sicherheitsniveau entsprechenden Personenidentifizierungsdaten (inklusive einer neu generierten E-ID-Registrierungsnummer) an den IdP.
5. Der IdP stellt die entsprechende E-ID aus – sorgt für die Aktivierung des Authentisierungsmittels und dessen Zuordnung zu der E-ID-Registrierungsnummer.



Figur 10 Ausstellung der Schweizer E-ID

Der IdP wird bei jedem Einsatz der E-ID involviert sein (vgl. Figur 11):

1. Eine Person will bei einem Dienstleister mit der E-ID Dienstleistungen beziehen.
2. Der Dienstleister leitet die Daten zur Person zur Authentisierung an den IdP weiter und spezifiziert die verlangten Attribute. Der Dienstleister kann dabei alle Identitätsattribute oder auch nur einige von ihnen (z.B. das Alter) verlangen.
3. Der IdP authentifiziert die Person mit Hilfe der E-ID und holt deren Einverständnis für die Übertragung der verlangten Attribute an den Dienstleister.
4. Der IdP überträgt die verlangten Attribute an den Dienstleister.
5. Die Person kann nun die Dienstleistung beziehen.



Figur 11 Einsatz der Schweizer E-ID

Jede E-ID soll unabhängig vom Aussteller bei allen Relying Parties eingesetzt werden können, sofern sie das von der Relying Party geforderte Sicherheitsniveau erfüllt. Damit dies möglich ist, selbst wenn eine Relying Party die Identifizierungsdienste bei einem anderen IdP bezieht, müssen die IdP interoperable Schnittstellen bereitstellen, über die Authentication-Requests und Identity-Assertions weitergeleitet werden können. Das Gesetz spezifiziert nicht, ob die Identity-Assertions Ende-zu-Ende verschlüsselt sein müssen. Ohne Zusatzmassnahmen besteht das Risiko, dass können somit nicht nur der IdP meiner Wahl und der Dienstleister, dem ich explizit mein Einverständnis erteilt habe, meine Daten einsehen. Auch alle anderen von der Relying Party akzeptierten Identitätsdienstleister können die Requests und Assertions lesen.

8_ Zusammenfassung

Abschliessend sind die wichtigsten Punkte zur Identifizierung in der digitalen Welt und zum Schweizer E-ID-Ansatz zusammengefasst:

1. **Identifizierung in der realen Welt bedeutet bei Behörden (im Government Umfeld) fast immer, dass die staatliche, rechtsgültige Identität einer Person verifiziert wird,** indem die Person physisch vor Ort ist und ausgebildetem Personal ein hoheitliches Dokument (ID-Karte, Pass) vorzeigt. Die Überprüfung der Identität erfolgt im Wesentlichen anhand des Gesichtsbildes im Ausweis.

2. **Identifizierung in der virtuellen Welt bedeutet in den meisten Fällen, dass eine selbstdeklarierte Identität mit Attributen wie Benutzernamen oder E-Mail-Adressen verifiziert wird**, indem eine Authentisierung anhand von Wissen, Besitz oder Sein (Biometrie) erfolgt. Mit der fortschreitenden Verlagerung der Geschäftsprozesse in den digitalen Raum sehen sich die Benutzer mit immer mehr Passwörtern und anderen Authentisierungslösungen konfrontiert.

3. **Falls in der virtuellen Welt die staatliche Identität einer Person gefordert ist (z.B. bei einer Online-Kontoeröffnung), findet die Identitätsprüfung in der Schweiz immer noch ausschliesslich anhand der physischen Dokumente statt, deren Echtheit und Besitzer optisch überprüft werden müssen.** Diese optische Prüfung ist im virtuellen Raum aufwändiger und weniger sicher als in der realen Welt. Staatlich anerkannte elektronische Identifizierungsmittel (E-ID) sollen unter Verwendung moderner Technologien digitale Identitätsprüfung sicherer und einfacher machen.

4. **Die gemäss Schweizer E-ID-Gesetz vorgesehene Lösung liefert die staatliche, rechtgültige Identität einer Person in der virtuellen Welt.** Sie zielt vor allem auf den Behörden-, Finanz- und Versicherungsbereich bzw. E-Government ab. Ob sie sich auch für Anwendungen mit selbstdeklarierter Identität durchsetzen wird, ist höchst fraglich.

5. **Die gemäss Schweizer E-ID-Gesetz vorgesehene E-ID wird allerdings nicht in die vom Staat ausgegebene ID-Karte integriert.** Die E-ID benötigt daher einen aufwendigen Registrierungsprozess. Dadurch, dass die E-ID von privaten IdP betrieben wird, der Staat aber bei der Ausstellung involviert ist, benötigt es bei der Registrierung sogar zwei Identitätsprüfungen: Zuerst überprüft der IdP die Identität des Antragstellers mit Hilfe eines physischen Ausweises. Danach muss sich der Antragsteller auch noch beim Bund Identifizieren, damit er dort sein Einverständnis mit der Übertragung seiner Daten an den IdP bekunden kann. Es ist nicht klar, wieso sich die Schweiz für die Lösung mit einem IdP und nicht für eine zertifikatsbasierte in die ID-Karte integrierte Lösung (wie in Estland oder Deutschland) entschieden hat.

6. **Bei der Lösung gemäss Schweizer E-ID-Gesetz ist zu beachten, dass alle IdP theoretisch in der Lage sind, Identitätsdiebstahl zu begehen oder neue Identitäten zu produzieren,** und zwar unabhängig davon, ob eine Person je eine bestimmte E-ID

beantragt hat oder nicht. Es wurde nicht der Ansatz «Security by Design», sondern «Security by Law» gewählt, d.h. es ist nicht ein sicheres Konzept erstellt worden, sondern man will die Sicherheit aufgrund von Gesetz und Vorschrift sicherstellen. Die damit verbundene Gefahr von Identitätsdiebstahl ist besonders bei der staatlichen, rechtsgültigen Identität beunruhigend. Ferner erfüllt das E-ID-Konzept auch den heute immer häufiger geforderten «Privacy by Design» Ansatz nicht.

Das Schweizer E-ID-Gesetz soll in erster Linie dem Bund bei der Digitalisierung seiner Dienste helfen. Die E-ID ist kein Ersatz für Identitätskarte oder Pass, sondern eine Software, welche auf Smartphones und Rechner geladen werden muss. Damit dürften mittelfristig gewisse Interaktionen mit dem Staat, bei denen man sich bisher mit Identitätskarte oder Pass ausweisen musste, sicherer und einfacher werden. Vielleicht werden auch einige staatsnahe Dienste und Finanzinstitute die E-ID für die Identifizierung von Kunden nutzen. Dass sich die E-ID auch als Ersatz für Passwörter beim Zugang zu anderen kommerziellen Diensten im Internet durchsetzen wird, ist wenig wahrscheinlich. Die aktuell schon auf Android und iPhone Smartphones, in Browsern oder über spezielle Passwortmanagerprogramme verfügbaren Lösungen sind einfacher und bereits heute weltweit einsetzbar. Ferner ist bei diesen Lösungen– im Gegensatz zur E-ID – auch klar was sie kosten.

9_ Literatur

(1. Juni 2018). *Botschaft zum Bundesgesetz über elektronische Identifizierungsdienste.* Von https://www.admin.ch/opc/de/federal-gazette/2018/3915.pdf abgerufen

(22. Juni 2001). *Bundesgesetz über die Ausweise für Schweizer Staatsangehörige (Ausweisgesetz, AwG).* Von https://www.admin.ch/opc/de/classified-compilation/19994375/201801010000/143.1.pdf abgerufen

(27. September 2019). *Bundesgesetz über elektronische Identifizierungsdienste (E-ID-Gesetz, BGEID).* Gesetz. Von https://www.admin.ch/opc/de/federal-gazette/2018/3989.pdf abgerufen

(18. März 2016). *Bundesgesetzüber Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES.* Von https://www.admin.ch/opc/de/classified-compilation/20131913/202001010000/943.03.pdf abgerufen

(2017). *Digital Identity Guidelines.* NIST. Von https://pages.nist.gov/800-63-3/ abgerufen

(23. Juli 2014). *EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt [eIDAS Verordnung EU Nr. 910/2014].* Von https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910&from=EN abgerufen

Hirter, C., Braun, N., Langhart, M., & Gmünder, M. (August 2016). *Evaluation Projekt SuisseID 2009-2015.* Institut für Wirtschaftsstudien Basel (IWSB). Staatssekretariat für Wirtschaft SECO. Von https://www.wbf.admin.ch/wbf/de/home/dokumentation/nsb-news_list.msg-id-64983.html abgerufen

Laube-Rosenpflanzer, A., Hassenstein, G., & Kunz, M. (13.09.2017). *Qualitätsmodell zur Authentifizierung von Subjekten.* Von http://ech.ch/de/standards/48092 abgerufen

Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., & Mortimore, C. (2014). *OpenID Connect Core 1.0.* Von https://openid.net/specs/openid-connect-core-1_0.html abgerufen

Vapen, A., Carlsson, N., Mahanti, A., & Shahmehri, N. (26 February 2016). *A Look at the Third-Party Identity Management Landscape.* IEEE Internet Computing Volume: 20, Issue: 2. doi:10.1109/MIC.2016.38

Wikipedia. (kein Datum). *Estonian identity card*. Abgerufen am 7. Dezember 2020 von https://en.wikipedia.org/wiki/Estonian_identity_card