Eidgenössisches Justiz- und Polizeidepartement (EJPD)
Bundesamt für Justiz
Bundesrain 20
3003 Bern

Per Mail zugestellt an: E-ID@bj.admin.ch

Zürich, 7. Oktober 2021

Öffentliche Anhörung zum Diskussionspapier zum «Zielbild E-ID»

Sehr geehrte Frau Bundesrätin

Sehr geehrte Damen und Herren,

In dieser Stellungnahme beziehen wir uns auf die am 02. September 2021 eröffnete öffentliche Anhörung des Eidgenössischen Justiz- und Polizeidepartements (EJPD) zum Diskussionspapier «Zielbild E-ID». Wir bedanken uns für die Konsultation in dieser wichtigen Angelegenheit.

Der Verband **Swiss Fintech Innovations** (SFTI, www.swissfintechinnovations.ch) vertritt die Interessen seiner Mitglieder (hauptsächlich Schweizer Banken und Versicherungen) im Bereich der Digitalisierung und Innovation in der Finanz- und Versicherungsindustrie. Unsere Arbeitsgruppe Regulations beschäftigt sich mit Gesetzgebung und Regulierung rund um diese Themengebiete.

Unserer Meinung nach wird sich der gesellschaftliche Konsens in Richtung Ambitions-Niveau 3 und Self-Sovereign Identity (SSI) entwickeln. Dies ist gleichbedeutend mit einem umfassenden Ökosystem digitaler Beweise und geht einher mit einer gesamtheitlichen digitalen Integration vieler verschiedenen Dokumente. Unseres Erachtens ist der SSI-Ansatz den anderen vom Bund vorgestellten Ansätzen überlegen.

Die Schweizer Variante sollte grundsätzlich der europäischen Variante der elektronischen ID, der EUid, interoperabel sein. Dies schafft EU-weite Anerkennung und somit europaweite Nutzbarkeit der Schweizer Lösung. Da der Prozess der Überarbeitung der betreffenden eIDAS-Richtlinie noch nicht abgeschlossen ist, ist ein konkreter Bezug auf die EU-Lösung derzeit zwar noch nicht möglich, jedoch sind die Arbeiten zu koordinieren. Darüber hinaus sollte auch die Interoperabilität mit nicht-EU-Ländern, wie beispielsweise UK oder der USA und deren Identitäts-Ökosystemen im Auge behalten werden. Neben Zusammenarbeit und Kooperation innerhalb eines Landes und zwischen den Ländern ist dementsprechend auch die Koordination mit globalen Standards wichtig.

Wir sind überzeugt, dass die E-ID mehrere Vorteile gegenüber den konventionellen Identifizierungs-mechanismen aufweist. Deswegen wollen wir im Folgenden die drei im Diskussionspapier genannten Fragen klären, auf mögliche Vorteile einer staatlich anerkannten Lösung eingehen und Vorschläge einbringen, wie man den offenen Fragen zum SSI-Ansatz begegnen könnte.

Wo sehen Sie den besonderen Nutzen der E-ID und welche Anwendungsfälle stehen für Sie im Vordergrund?

Unser Alltag wird zunehmend digital. Dieser Wandel geschieht nicht stetig, sondern dessen Geschwindigkeit nimmt kontinuierlich zu. In dieser Hinsicht wird es immer wichtiger, dass unser

„digitales Gegenüber“ ausreichend identifiziert ist. Dies muss auf Basis einer gesetzlich anerkannten Lösung möglich sein. Nur eine solche schafft massengeschäftstaugliche Rechtssicherheit. Eine solche "Vertragssicherheit" muss auch im Zeitalter der Digitalisierung gewährleistet werden. Mithilfe der Einführung einer staatlich anerkannten elektronischen Identität könnte im Idealfall eine umfassende Lösung geboten werden. Ziel muss sein, dass sich Schweizer Bürgerinnen und Bürger sowie Firmen eindeutig, sicher und benutzerfreundlich digital ausweisen können.

Mithilfe der E-ID könnten **Behördengänge**, beispielsweise bei der Einholung notwendiger Dokumente zur Gründung einer Firma, die Bestellung des Betreibungsregisterauszugs oder die Durchführung grundbuchlicher Transaktionen effizienter sowohl für die Behörden als auch für einzelne Bürger gestaltet werden. Ferner erhöht sich die **Sicherheit bei Geschäftsbeziehungen**, da Geschäftspartner und Kunden mit hoher Sicherheit identifiziert werden können.

Die Grundlage eines jeden wirtschaftlichen Erfolgs besteht darin, dass die betreffenden Vertragsparteien sich gegenseitig vertrauen. Da sich unsere Prozesse und Dienstleistungen immer stärker in den digitalen Raum verschieben, benötigen wir einen sicheren Zugriff auf unsere Daten. Sowohl Unternehmen als auch deren Kunden würden von einer digitalen Identifikation profitieren. Alltägliche Prozesse wie beispielsweise digitale Vertragsabschlüsse oder Einkäufe, sowie das **KYC («Know-Your-Customer»)** könnten durch die E-ID starke Effizienzsteigerungen erfahren. Des Weiteren sind wir überzeugt, dass die elektronische Identität den Weg für weitere, bisher noch unbekannte, technische Lösungen ebnet.

Aus parlamentarischer Perspektive würde die Schaffung einer E-ID beispielsweise die Umsetzung der folgenden Motionen unterstützen bzw. ermöglichen:

a) Motion 21.3180 Vollständig digitale Unternehmensgründung sicherstellen von NR Andri Silberschmidt (FDP, Zürich) vom 16.3.2021

und

b) Motion 20.4356 Digitaler Fahrzeug- und Führerausweis von NR Franz Grüter (SVP, Luzern); vom 30.11.2020

Vorgenannte Ausprägungen sind nur beispielhaft zu verstehen. Digitale Prozesse sind gegenüber "physischen" generell wesentlich effizienter, rascher und kostengünstiger, was letztlich auch dem Kunden bzw. Konsumenten zu Gute kommt. Eine gesetzlich anerkannte E-ID ist letztlich notwendige Grundlage für jede digital angebotene Dienstleistung des Staates und für jedes digital angebotene Geschäftsmodell der Wirtschaft. Innovation wird insbesondere auch durch Wettbewerb gefördert. Daher halten wir es für wichtig, dass die Möglichkeit besteht, dass sich mehrere ID Anbieter etablieren können, die die staatlichen Vorgaben erfüllen und entsprechend zertifiziert werden. Eine gesetzlich anerkannte E-ID unterstützt damit nachhaltig Innovationskraft und damit auch Attraktivität des Wirtschaftsstandorts Schweiz.

Welches sind für Sie die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

Der **Zugang** zu, der **Zugriff** auf und die **Nutzung** der E-ID muss für die User ohne nennenswerte Schwierigkeiten, möglichst bequem und trotzdem sicher, gewährleistet werden. Die weite Akzeptanz und die einhergehende fortschreitende Digitalisierung unserer Gesellschaft wird nur dann vorhanden sein, wenn die Aspekte der einfachen und raschen Erhältlichkeit, der **Benutzerfreundlichkeit** und der **Transparenz**, insbesondere zur Wahrung des Vertrauens, greifbar sind.

Die drei wichtigsten, hier beschriebenen, Anforderungen sind: **Zugänglichkeit**, **Benutzer-freundlichkeit** und **Transparenz**. Zugänglichkeit und Benutzerfreundlichkeit sind aus unserer Sicht eng miteinander verbunden. Transparenz ist aus unserer Sicht insbesondere auch eine Aufgabe der begleitenden Kommunikation; weniger eine Anforderung an die Lösung selbst.

Ergänzend sehen wir die **Fokussierung auf privatwirtschaftliche Anwendungsbereiche** und die Schaffung allgemeingültiger Richtlinien, die den **Wettbewerb** zulassen und fördern, als wichtige Anforderungen für ein nachhaltiges ID Ökosystem.

Der *erste* Punkt des **einfachen Zugangs, Zugriffs und Nutzung** impliziert, dass die gesamte Schweizer Bevölkerung in der Lage sein muss, auf ein staatlich anerkanntes elektronisches Identifikationsmittel zurückgreifen zu können. Die rasche Durchdringung der Schweizer Bevölkerung in den ersten Monaten der Verfügbarkeit wird sich als unabdinglich erweisen in der erfolgreichen Integration der E-ID.. Die administrativen Prozesse zum Erhalt der E-ID sollten also kurz und unkompliziert gestaltet werden. Das Login sollte so intuitiv und zeiteffizient sein, dass eine grosse Zahl Nutzer innerhalb kürzester Zeit die Plattform der E-ID benützt. Jedoch darf damit unter keinen Umständen ein Minus bei Sicherheit und Integrität der E-ID einhergehen.

Zweitens ist es für die Akzeptanz der E-ID essenziell, dass eine **hohe Benutzerfreundlichkeit** besteht. Das User Interface sowie der Identifikationsprozess müssen übersichtlich sein. Ferner muss ein Ziel der Einführung der E-ID sein, dass es ohne lange Übergangsperiode allfällig notwendige Behördengänge auf Gemeinde- und auf Bundesebene ersetzt. Ferner sollten Unternehmen sowie Privatpersonen nicht durch unnötige Komplexität der einzelnen Funktionen bei der Einführung der E-ID überwältigt werden. Die Abwicklung von Geschäftsprozessen (z.B. Verträge) und alltäglichen Transaktionen (z.B. der Kauf eines ÖV-Tickets oder die Bestellung eines Betreibungsregister-auszugs) muss schnell und unkompliziert vonstattengehen. Des Weiteren wird es wichtig sein, eine Vereinheitlichung und Kompatibilität der E-ID zumindest auf europäischer Ebene anzustreben. Zusätzlich wird die Nutzerakzeptanz durch eine hohe Alltagsrelevanz sichergestellt. Hierzu ist eine breite privatwirtschaftliche Akzeptanz mit Anwendungsfällen über behördliche Anwendung hinaus essenziell.*Drittens* muss der Bund für **Transparenz und Verständnis** der Materie sorgen, denn nur so kann das notwendige Vertrauen der Bevölkerung in die neuartige Identifikationsmöglichkeit entstehen. Dazu gehört auch, die verschiedenen Rollen von Staat und Wirtschaft innerhalb des "Systems" einer E-ID darzustellen, ebenso wie die Tatsache, dass solche verschiedenen Rollen für das Funktionieren des Gesamtsystems notwendig sind. Die Vorteile der E-ID sowie dessen Funktionsweise sollten konsequent aufgezeigt werden. Allfällige Ängste der Bevölkerung, dass eine elektronische Identität in Richtung eines digitalen Überwachungsstaates geht, müssen von Anfang an proaktiv unterbunden werden. Ein wiederverwendbarer digitaler Identitätsservice ist nicht möglich ohne das klare Verständnis, Vertrauen und Engagement eines jeden Benutzer.

Welchen Nutzen sehen Sie in einer nationalen Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Nachweise (z.B. E-ID, digitaler Führerausweis, Mitarbeiterausweise, Ausbildungsnachweise) auszustellen und überprüfen zu können?

Die **Sicherheit** vieler Anmeldeverfahren wird oftmals reduziert, indem Passwörter z.B. mehrfach verwendet oder sogar aufgeschrieben werdenMit einer digitalen Infrastruktur könnten die Schweizer Bevölkerung alle persönlichen Unterlagen in einem einzigen digitalen Wallet speichern und dieses jederzeit auf Abruf vorweisen oder übermitteln. Um Innovation und Wettbewerb zu fördern, sollten aber wie erwähnt verschiedene digitale Wallets zugelassen werden. Die Kundenbeziehungen könnten so einfacher überprüft und abgeschlossen werden. Essenziell bleibt,

dass bei jeder Verwendung die Wahl bestehen muss, welche Informationen der Gegenpartei zur Verfügung gestellt werden sollen und welche nicht. **Der elektronische Geschäftsverkehr würde somit sicherer werden und die Privatsphäre eines Einzelnen besser gewahrt werden können** Dafür ist es notwendig, verschiedenste digitale Nachweise sicher speichern und teilen zu können. Vielfältige Anwendungsmöglichkeiten im Privatsektor stellen die Relevanz der E-ID sicher. Die nationale Infrastruktur kann darüber hinaus die Basis dafür bilden, dass sich jeder Mensch und jedes Unternehmen **europaweit online und offline ausweisen** kann und bestimmte persönliche Informationen nachgewiesen werden können, wenn die Interoperabilität mit entsprechende EU-Lösungen gesichert ist.

Wie ordnen wir die im Diskussionspapier erwähnten Nachteile zum SSI-Ansatz ein?

Die SSI kann als derzeit komplexeste Entwicklungsstufe digitaler Identitäten gesehen werden. Das Ziel der SSI ist, die Probleme und Herausforderungen der existierenden Identitätsverwaltungssystemen zu lösen. Die Nachteile bei der Umsetzung der SSI-Prinzipien hängen dabei von der konkreten technischen Umsetzung ab. Eine technologie-offene, ergebnisorientierte Definition der Ziele der E-ID ermöglicht die Umsetzung mit den an den besten geeigneten technologischen Lösungen.

Zwar ist der SSI-Ansatz neu und unbekannt. Trotzdem ist zu beachten, dass **der SSI-Ansatz die möglichen Entwicklungsstufen der beiden alternativen Ansätzen (Public-Key-Infrastruktur und zentraler staatlicher Identitätsprovider) vorwegnehmen würde.** Es ist denkbar, dass eine Einführung mit Verzicht auf die Implementierung eines kompletten Ökosystems im Nachhinein als nicht ausreichend betrachtet werden wird. Dies könnte nämlich genau dann geschehen, wenn die umfassenden Vorteile den Usern ersichtlich werden.

Unserer Ansicht nach ist der SSI-Ansatz den anderen vom Bund vorgestellten Ansätzen überlegen. Ferner sind wir überzeugt, dass das Bewusstsein über dessen Fähigkeiten zügig entstehen wird. Die Voraussetzung dafür ist lediglich die lückenlose, unkomplizierte und ganzheitliche Implementierung des Ansatzes. Als ersten Schritt sollten dementsprechend noch offene Grundsatzfragen und Standards geklärt und erläutert werden.

Ein SSI-System basiert auf einem **dezentralen Ansatz.** Die Verantwortung zur Verwaltung der Identität (verified credentials) liegt bei dem einzelnen User und lässt nur wenig Hilfestellung zu. Unter kritischer Betrachtungsweise könnte man meinen, dass dies Unsicherheit auslöse und Wege zur Manipulation eröffne. Dem muss durch eine starke Governance vorgebeugt werden. Durch ein Zertifizierungssystem für Issuer kann beispielsweise Identitätsmissbrauch abgewehrt werden. Zusätzlich können Wallet-Provider dem User Hilfestellung bei der Anwendung der E-ID leisten. Um das Problem der forensischen Aufklärungsschwierigkeiten zu lindern, könnte man auf die bereits bekannte und oftmals verwendete **2-Faktor-Authentifizierung** zurückgreifen.

Offene Fragen zum SSI-Ansatz

Welche Governance-Ebenen gibt es und wer ist dafür zuständig (z. B. Governance-Ebenen nach Trust over IP Framework: Ökosystem, Credentials, Provider, Utility)?

Generell betrachtet, sorgt eine gute Governance für mehr Sicherheit, indem Verfahren und Rechenschaftspflicht vorgesehen werden. Governance ist besonders für die universelle Interoperabilität von entscheidender Bedeutung, da alle Teilnehmer des Netzwerks in der Lage sein müssen, selbst zu entscheiden, wem und was sie vertrauen wollen. Die **vier Ebenen des «Trust-**

over-IP-Frameworks» erscheinen im Zusammenhang mit einer SSI sinnvoll. Auf jeder Ebene bedarf es einer Publikation des erstrebten Governance-Frameworks.

Auf der *ersten Ebene* sollte der Bund und die von ihm zertifizierten Parteien ihre verschiedenen Zuständigkeiten erarbeiten. Bei der Erstellung der Governance des gesamten Ökosystem sollten möglichst viele Parteien involviert werden. Auf der *zweiten Stufe* sollte der Staat nur noch das Registry für staatlich beauftragte Aufgaben übernehmen (Pass, Führerschein etc.) und genügend Raum lassen für externe Ersteller von Registries. Gleichzeitig muss aber sichergestellt werden, dass die verschiedenen Systeme untereinander interagieren und die Governance untereinander abgestimmt wird. Auf der *dritten und vierten Ebene* können ein höherer Grad an Autonomie bestehen. Solange die Funktionsweise nicht beeinträchtigt wird, sollte aktiv dafür gesorgt werden, dass verschiedene Lösungen angeboten werden. Mit Blick auf die grossen Unterschiede zwischen verschiedenen Arten von Dienstleistungen oder Geschäftsmodellen ist dies ebenso sinnvoll wie notwendig. **Das Governance-Framework sollte zwar bestimmte Mindestvorgaben erfüllen, schlussendlich sollen sich aber die Lösungen durchsetzen, die am wettbewerbsfähigsten sind. Zu diesem Zweck muss der Aufbau der Governance nach bewährtem Schweizerischen Ansatz prinzipien- und risikobasiert sowie proportional (verhältnismässig) und überdies wettbewerbs- und technologieneutral erfolgen.** Gestützt darauf können effiziente Dienstleistungs- und Geschäftsmodelle entwickelt werden, welche den konkreten Verhältnissen gerecht werden und z.B. je nach Umfang, Komplexität und Risiko auch unterschiedliche Sicherheitsstandards zum Einsatz bringen können.

Muss der Staat auf gewissen Komponenten das Monopol haben? Müssen Wallets staatlich zertifiziert werden? Wird die Auswahl von Wallet und Institutional Agent dem User überlassen? Gibt es eine Regelung, welche Teile kooperativ, welche in Konkurrenz erstellt und betrieben werden?

Wir sind der Ansicht, dass sich die digitale Identität **nutzerzentriert** gestaltet sein muss. Das bedeutet, dass sie dem Einzelnen gehört, von ihm verwaltet und kontrolliert wird. Damit die digitalen Interaktionen funktionieren, müssen die beteiligten Organisationen die digitale Identität **akzeptieren**.

Deswegen schlagen wir vor, dass **gewisse sicherheitsrelevante Komponenten weiterhin einer monopolistischen Kontrolle des Staates** bedürfen, darunter fallen beispielsweise das Ausstellen von Pässen oder Führerscheinen. Die Delegation dieser Autorität wäre kritisch zu betrachten und sicherlich nicht förderlich für den Aufbau des Vertrauens der User in die E-ID. Hingegen sollten nicht-staatlich angebotene Dienstleistungen nicht zwingend von staatlichen Behörden ausgestellt werden müssen. Es macht keinen Sinn, Kinotickets und Zooeintritte als ähnlich essenziell zu betrachten wie Reisepässe und Führerscheine.. Dementsprechend müsste der Staat nicht als Issuer von jeglichen Dokumenten des gesellschaftlichen Lebens fungieren.

Die E-ID sollte zulassen, dass **mehr als ein Wallet** für digitale Identitäten verwendet werden kann. D.h., dass Wallets **frei wählbar** sein sollten und nicht staatlich zur Verfügung gestellt werden müssen. Die Wallets sollten selbstverständlich interoperabel und somit wettbewerbsfähig sein. Als Folge sollte ein innovativer Markt entstehen, der den Bedürfnissen der Verbraucher am besten gerecht wird. Es erscheint trotzdem sinnvoll, eine **staatliche Zertifizierung** für Wallets anzubieten, um das Vertrauen in das digitale Wallet zu erhöhen. Des Weiteren können einzelne kantonale Behörden die Rolle des Wallet-Anbieters wahrnehmen werden, um ihrer Bevölkerung z.B. massgeschneiderte Services anzubieten.

Die Stufe der einzelnen **Verifier benötigt keine staatliche Autorität** beispielsweise zur Kontrolle der Gültigkeit der einzelnen Dokumente. Ähnlich wie beim Covid-Zertifikat würde lediglich ein Abgleich stattfinden, um die Gültigkeit zu überprüfen.

Wer betreibt die Registry? Ist eine eigene, nationale Registry nötig oder schliesst man sich einem bestehenden, internationalen Ökosystem an? Wollen oder sollen Kantone, Städte oder private Unternehmen Speicher-Knoten (Nodes) betreiben dürfen? Welche Technologie wäre zu bevorzugen? Welche Rolle spielt die Datenmenge? Wie löst man Interoperabilitätsfragen zu anderen Registries? Besteht für den Issuer sogar die Wahlfreiheit der Registry?

Das Covid-Zertifikat zeigt auf, dass eine europaweite Gültigkeit einer Registry möglich ist. Jedes teilnehmende Land sollte also dafür sorgen, dass **mindestens eine staatliche Registry** zur Verfügung steht. Trotzdem sollte man sich nicht auf eine einzelne Registry pro Staat verlassen und **auch weitere, dezentrale Nodes** zulassen. Dies sollte auch dann zutreffen, wenn Länder verschiedene Identifizierungstechnologie verwenden.

Solange die Datensicherheit gewahrt bleibt, sollte **keine Einschränkung bezüglich Anbieter von Registries** bestehen. Diese Anbieter können entweder kantonal, städtisch oder privat finanziert zur Verfügung gestellt werden und sollten zum Ziel haben, das Vertrauen in das Ökosystem zu erhöhen. Des Weiteren sollte das Registry für nicht-staatlich angebotene Dokumente frei wählbar sein. Letzteres impliziert aber, dass **jeder einzelne Node zertifiziert** und gelegentlich überprüft werden sollte.

Wer darf Issuer sein? Bleibt das System völlig offen zum Gewinn zusätzlicher Anwendungsfälle oder werden die Issuer spezifisch ausgewählt oder berechtigt?

Um die Legitimation und Anwendung des digitalen Ausweises zu fördern, sollten die Limitierungen des Systems möglichst gering sein. Eine **Dezentralisierung der Befugnis zur Ausstellung** erscheint sinnvoll. Diesbezüglich sollten die Kontrolle und Übersicht über das Ausstellen von digitalen Dokumenten aber nicht abgegeben werden. Bevor beispielweise eine dezentrale Partei die Lizenz zur Ausstellung eines digitalen Dokuments erhielte, sollte es von einer staatlichen Partei **zertifiziert** werden.

Wie werden Backups und Transfers von Credentials ermöglicht? Wie können zentrale Backups und damit attraktive Hacker-Angriffsziele vermieden werden? Welche Rolle spielt eine mögliche kryptografische Verbindung zwischen Wallet und Verified Credentials?

Wir schlagen vor, dass eine **Verpflichtung** zur kryptografischen Verschlüsselung für alle E-ID-Beteiligten bestehen sollte. Das Vertrauen der User kann nur dann erhalten werden, wenn für eine sichere Handhabung der persönlichen Daten gesorgt wird. Es ist deshalb ratsam, regelmässige Kontrollen zur Verhinderung oder Aufdeckung von Betrug einzurichten.

Welche Sicherheitsmechanismen sind für den Zugriff zur Wallet nötig?

Wie bereits erwähnt könnte man hierbei auf eine **2-Faktor-Authentifizierung oder biometrische Verifizierung** mittels Fingerabdrucks oder Gesichtsscan zurückgreifen.

Wie können Verified Credentials auf mehreren Geräten benutzt werden? Wann wäre dies nötig? Reicht es, wenn mit dem einen Smartphone immer eine Verbindung zum Verifier aufgebaut werden kann, unabhängig davon, auf welchem anderen Gerät man gerade den nach der E-ID-fragenden Prozess initiiert hat?

Die gegenwärtig verfügbaren Möglichkeiten lassen es bereits zu, denselben Account auf mehreren Geräten zu verwenden. So könnte z.B. eine DLT-Lösung für die Protokollierung von **Mehrfach-Verwendungen** eingesetzt werden.

Wer definiert Credential-Schema, braucht es eine ausgewiesene Stelle zur Definition und Koordination (z. B. eCH) oder werden die Definitionen branchenabhängig entwickelt?

Die Definitionen sollten **branchenabhängig** entwickelt werden. Es ist zu empfehlen, diese **zentral zu hinterlegen**. Insbesondere im Falle eines Systemausfalls würde es sich als wichtig erweisen, ein Credential-Schema nicht nur an einem Ort abzuspeichern.

Benötigt es überhaupt einen staatlichen Authentifizierungsdienst? Wäre eine Verknüpfung von Ausstellungsprozess und Hinterlegen von Authentifizierungsfaktoren sinnvoll, um vom aufwändigen Identifikationsprozess bei der Ausstellung zu profitieren und um eine hohe Sicherheit beim Authentifikationsprozess zu ermöglichen?

Unserer Meinung nach ist die erstmalige Ausstellung einer staatlichen Identität (Führerschein, Pass etc.) die Aufgabe des Staates. Eine Verknüpfung von Ausstellungsprozess und Authentifizierungsfaktoren erscheint sinnvoll. Die Sicherheit könnte dadurch erhöht werden und Manipulationsversuchen vorgebeugt werden.

Gerne stehen wir Ihnen für eine vertiefte Diskussion und für die weitere Zusammenarbeit jederzeit gerne zur Verfügung.

Freundliche Grüsse

Sig. Werner W. Wyss	Sig. Prof. Dr. Cornelia Stengel	Sig. Philipp Rosenauer
Leiter Arbeitsgruppe Regulations	Co-Director/Mitglied Arbeitsgruppe Regulations	Mitglied Arbeitsgruppe Regulations