Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizi Departement EJPD
Bundesamt für Justiz BJ

7. März 2024

Konsultation zum Technologie-Entscheid betreffend Vertrauensinfrastruktur und E-ID

Zusätzliche Stellungnahmen

Appenzell Ausserrhoden

Departement Finanzen

Obstmarkt 3
9102 Herisau
Tel. +41 71 353 61 11
Finanzen@ar.ch
www.ar.ch

Departement Finanzen, 9102 Herisau

Bundesamt für Justiz
Bundesrain 20
3003 Bern

Hansueli Reutegger
Regierungsrat
Tel. +41 71 353 68 10
hansueli.reutegger@ar.ch

Zustellung per E-Mail an: E-ID@bj.admin.ch

Herisau, 15. Januar 2023

Eidg. Konsultation; "E-ID-Technologie-Entscheid"; Stellungnahme

Sehr geehrte Damen und Herren

Am 1. Dezember 2023 hat das Bundesamt für Justiz eine Konsultation zum Technologie-Entscheid für die E-ID eröffnet. Gemäss Konsultationsunterlagen werden ein Szenario A (der technischen Richtung der EU folgen) und ein Szenario B (eigenständiger technologischer Pfad für die Schweiz) zur Diskussion gestellt. Für Appenzell Ausserrhoden nimmt das Departement Finanzen gerne wie folgt Stellung.

Die Staatskanzlei des Kantons Zürich hat beim Europa-Institut der Universität Zürich ein Kurzgutachten zu den sich stellenden europarechtlichen Fragen in Auftrag gegeben und nach Vorliegen den anderen Kantonen zur Verfügung gestellt. Es kommt im Ergebnis zum Schluss, dass die Konsultation der Bundesverwaltung zu einem verfrühten Zeitpunkt erfolge. Die Entwicklungen in der EU seien in massgeblichen Bereichen noch nicht abgeschlossen. Dies betreffe einerseits die technische Umsetzung der digitalen Identität und der hierbei verwendeten Spezifikationen sowie andererseits die Datenschutzstandards bei der hierbei auftretenden Verarbeitung personenbezogener Daten.

Das erwähnte Kurzgutachten bestätigt den Eindruck, den die Unterlagen beim Lesen ergeben. Die wichtigsten Fragen, die als Rückmeldung erwartet werden, lassen sich beim jetzigen Informationsstand kaum verlässlich beantworten. Im Kurzgutachten wird insbesondere darauf hingewiesen, dass namentlich zur Einhaltung von datenschutzrechtlichen Belangen durch die EU im gegenwärtigen Zeitpunkt keine abschliessende Beantwortung möglich sei. Dieser Haltung ist zuzustimmen. Appenzell Ausserrhoden beantragt, die Konsultation zu einem späteren Zeitpunkt erneut durchzuführen, wenn die massgeblichen Grundlagen für eine Beurteilung vorliegen.

Allgemein kann festgehalten werden, dass sich der Bund beim zweiten Anlauf für eine E-ID nicht von der Entwicklung in der EU abhängig machen sollte. Zentral ist, dass ein überzeugendes Projekt aufgegleist wird, das wenig Angriffsfläche bietet, bei einer Volksabstimmung besteht und das eine in der Schweiz breit akzeptierte E-ID bringt. Falls in der Schweiz in Zukunft das Bedürfnis entsteht, ebenfalls eine E-ID der EU einzusetzen, so dürften sich dafür dannzumal technische und rechtliche Lösungen finden. Die Konzentration sollte indessen auf dem E-ID-Projekt des Bundes liegen.

Freundliche Grüsse

Hansueli Reutegger, Vorsteher Departement Finanzen

Kopie an

- Regierungsrat (via Tischmappe)
- Departement Inneres und Sicherheit
- Kantonskanzlei
- AR Informatik AG

Von: Fischer Thomas, FIN-KAIO-Stab <thomas.fischer@be.ch>
Gesendet: Donnerstag, 11. Januar 2024 13:40
An: Rauschenbach Rolf BJ <rolf.rauschenbach@bj.admin.ch>; _BJ-E-ID <E-ID@bj.admin.ch>
Betreff: AW: Konsultation "Technologie-Entscheidung für die E-ID" - Verlängerung der Antwortfrist, Übersetzungen des Diskussionspapiers

Sehr geehrter Herr Rauschenbach, sehr geehrte Damen und Herren

Gerne nehme ich namens des Amtes für Informatik und Organisation des Kantons Bern (KAIO) innert erstreckter Frist Stellung zu Ihrem beiliegenden Diskussionspapier und danke Ihnen für die Gelegenheit zur Mitwirkung.

Die von Ihnen gestellten Fragen beantworten wir wie folgt:

Welches Szenario bevorzugen Sie? Und aus welchem Grund?

Aus unserer Sicht ist dies zurzeit noch nicht beurteilbar.

Die beiliegende Stellungnahme des Europainstituts an der Universität Zürich vom 21.12.2023 hält fest: «Im Ergebnis ist festzustellen, dass die Konsultation der Bundesverwaltung zu einem verfrühten Zeitpunkt erfolgt. Die Entwicklungen in der EU sind in massgeblichen Bereichen noch nicht abgeschlossen. Dies betrifft einerseits die technische Umsetzung der digitalen Identität und der hierbei verwendeten Spezifikationen sowie andererseits die Datenschutzstandards bei der hierbei auftretenden Verarbeitung personenbezogener Daten. (...) Grundsätzlich sollte eine international anschlussfähige Lösung bei der Einführung einer digitalen Identität im Interesse der Wirtschaft sowie auch im Interesse der Bürger im Vordergrund stehen. Wirtschafts- und Privatleben reichen heute über die Landesgrenzen hinaus; praktikable Identitätsnachweise spielen hierbei eine zentrale Rolle (...). Hiervon sollte nur abgewichen werden, wenn die EU tatsächlich von ihren eigenen, in der Datenschutz-Grundverordnung statuierten hohen Datenschutzstandards abweichen sollte.»

Dieser Meinung schliessen wir uns an. Wir schlagen daher vor, die Konsultation zu wiederholen, sobald die EU-Grundlagen beschlossen sind, wenn sie wider Erwarten ein Unterschreiten der Datenschutzanforderungen gemäss der DSGVO und des Schweizer Datenschutzrechts vorsehen.

Ist dies nicht der Fall, sollte sich die Schweizer E-ID an der EU-Lösung orientieren. Dies aus folgenden Gründen: Die Einführung der E-ID ist das wohl dringendste Bedürfnis der Digitalisierung der Verwaltungsabläufe in der Schweiz. Bei der Umsetzung sollte daher das risikoärmste und erfolgversprechendste Vorgehen gewählt werden, das mit den gesetzlichen Datenschutzvorgaben vereinbar ist. Dazu ist es erforderlich, dass auf technologische und regulatorische Ansätze abgestellt werden kann, die in der EU bereits erprobt sind. Zudem kann dies aufgrund der dadurch möglichen Wiederverwendung von Software auch Kosten sparen. Und nur dies stellt die Interoperabilität der E-ID mit digitalen Identitäten der EU sicher. Dies ist für die öffentliche Verwaltung wichtig, wenn es darum geht, Geschäftsprozesse zu digitalisieren, die auch ausländische Personen mit einbeziehen (als Steuerzahlende, Lieferanten, etc.). Auf eine teure und risikoreiche «Helvetisierung» bzw. einen «Swiss Finish» sollte u.E. daher verzichtet werden.

Erfüllen beide Szenarien Ihre Erwartungen? (Ja/Nein)

Nein.

Welche grossen Risiken sehen Sie?

Aufgrund der Ausführungen zur ersten Frage sind die beiden Varianten und ihre Risiken u.E. noch nicht beurteilbar.

Welche «roten Linien» sollten nicht überschritten werden? Wo ist für Sie kein Kompromiss denkbar?

Aufgrund der Ausführungen zur ersten Frage ist dies u.E. noch nicht beurteilbar.

Zusätzliche Bemerkungen

Diese Umfrage wurde an die Kantonsregierungen adressiert. Weil die angesetzte Antwortfrist für eine Befassung des Regierungsrates zu kurz ist, gibt diese Antwort die Fachmeinung des im Kanton Bern zuständigen KAIO wieder, und nicht notwendigerweise die Meinung des Regierungsrates.

Freundliche Grüsse

Thomas M. Fischer, Rechtsanwalt, stv. Amtsleiter, Leiter Stab / Fachbereich Recht
+41 31 633 40 94 (direkt), +41 79 746 75 03 (Mobile), thomas.fischer@be.ch
Finanzdirektion des Kantons Bern, Amt für Informatik und Organisation, Stab Amtsleitung
Wildhainweg 9, 3012 Bern
+41 31 633 59 00, info.kaio@be.ch, www.be.ch/kaio

REPUBLIQUE ET CANTON DE GENEVE
Département des institutions et du numérique
La Conseillère d'Etat

DIN
Case postale 3952
1211 Genève 3

Monsieur Rolf Rauschenbach
Office fédéral de la justice
Bundesrain 20
3003 Berne

Aigle 400151-2024

Genève, le 22 janvier 2024

Concerne : Consultation sur la décision technologique

Cher Monsieur,

Le Conseil fédéral a transmis le 22 novembre dernier son projet de loi et le message relatifs à la nouvelle loi fédérale sur la preuve d'identité électronique et les autres preuves électroniques (Loi sur l'e-ID, LeID). Le Conseil fédéral souhaite délivrer les premières e-ID dans les meilleurs délais et si possible dès l'entrée en vigueur de la loi. Je me réjouis de ces avancées.

Afin de rendre cela possible, l'Office fédéral de la justice consulte, de manière informelle, les acteurs de l'écosystème engagé dans la réalisation de cette e-ID et de l'infrastructure de confiance, dont le canton de Genève. Par ce courrier, je réponds donc aux questions que vous avez mises en consultation. En parallèle de ce courrier, les réponses ci-dessous seront intégrées au formulaire en ligne ad hoc.

1. *Quel scénario préférez-vous ? Et pour quelle raison ?*

Nous exprimons une préférence pour le scénario B, qui permet une meilleure protection de la vie privée et une autonomie stratégique renforcée pour la Suisse par rapport au scénario A. A cet égard, je rappelle que le corps électoral du canton de Genève a voté à plus de 94% en juin 2023 l'introduction d'un nouveau droit fondamental à l'intégrité numérique, illustrant les attentes fortes de protection de la part de la population. La confiance est en effet un fondement du succès de l'eID et le scénario B permet, à notre lecture, de mieux l'assurer.

Toutefois, il convient de relever que le scénario A présente des avantages significatifs en termes de compatibilité et d'interopérabilité avec les systèmes prévus par l'Union européenne, ce qui peut accélérer l'implémentation et l'adoption, particulièrement dans le contexte des activités poursuivies par les entreprises.

2. *Les deux scénarios répondent-ils à vos attentes ?*

Nous comprenons les enjeux de développements technologiques rapides et saluons le travail effectué par l'équipe du projet e-ID. L'accompagnement par des experts et les retours des scientifiques et de la société civile conforteront les choix de la Confédération. Selon les informations disponibles, les deux scénarios semblent répondre aux principales attentes.

Tout en privilégiant le scénario B pour son approche plus stricte en matière de confidentialité, nous recommandons cependant d'envisager une stratégie qui cherche à renforcer ces aspects au sein du scénario A. Une étude ou des essais complémentaires pourraient être envisagés afin de tendre vers une solution qui combine la facilité d'implémentation et l'adoption utilisateur du scénario A avec les normes élevées de confidentialité du scénario B. L'interopérabilité avec l'Union européenne devant être privilégiée pour adopter des standards communs pour l'ensemble des acteurs publics et économiques, facilitant l'émergence de nouveaux usages en Suisse et avec nos partenaires Européens.

Il conviendrait en effet de viser une solution e-ID qui soit à la fois fonctionnelle dans le contexte européen et qui respecte les valeurs de confidentialité que la Suisse cherche à préserver.

3. *Quels risques majeurs prévoyez-vous ?*

Compte tenu des investissements importants qui seront consentis dans cette infrastructure, de la lenteur à laquelle les e-ID seront mécaniquement créées, du caractère éminemment souverain de l'e-ID - au même titre que les documents actuels d'identité propres à la Suisse - et de la confiance permanente qu'il faudra créer et entretenir dans ce nouveau système, il est crucial de démarrer sur le scénario vu comme le plus pérenne.

Les principaux risques identifiés sont les suivants :

- Vu l'importance culturelle pour la population Suisse de pouvoir contrôler et limiter les possibilités de surveillance, les défauts du scénario A vis-à-vis des possibilités de traçage nous semblent risqués. Il suffirait seulement de quelques abus pour détruire la confiance, dont le risque qu'ils se produisent peut être considéré comme très élevé

- En matière de choix technologique, il s'agit de tout particulièrement faire attention aux algorithmes de chiffrement et s'assurer de la disponibilité des compétences, de la maitrise et des connaissances techniques des solutions déployées sans oublier en particulier de prendre en compte les travaux sur la « cryptographie post-quantique » afin de s'assurer de la pérennité des choix effectués.

- En ce qui concerne la mise en œuvre et l'interopérabilité, il est essentiel que la Suisse lance son e-ID dans un délai proche de celui du calendrier européen. De plus, il est important de poursuivre une démarche de standardisation et d'harmonisation des solutions techniques. Cela garantira la mise en place d'une solution homogène par toutes les parties prenantes, compatible tant avec les systèmes suisses qu'européens. En effet, un retard significatif dans sa mise en œuvre ou un manque d'interopérabilité pourrait s'avérer préjudiciable pour l'économie suisse.

4. *Quelles sont les "lignes rouges" à ne pas franchir ? Dans quels domaines aucun compromis n'est envisageable pour vous ?*

Le projet doit répondre aux intentions des motions politiques. La confiance de la population envers cet écosystème ést une base indispensable à sa réussite.

Je tiens à souligner ici combien l'approche retenue par la Confédération d'impliquer un écosystème large dans ces choix techniques de nature politique est exemplaire et vous en remercie.

Pour tout complément, le délégué au numérique du canton de Genève, M. Alexander Barclay (alexander.barclay@etat.ge.ch), est à votre disposition.

En vous remerciant pour votre sollicitation, je vous prie de recevoir, cher Monsieur, mes salutations distinguées.

Carole-Anne Kast

Von: Martin.Jenny@gl.ch <Martin.Jenny@gl.ch>
Gesendet: Donnerstag, 14. Dezember 2023 17:04
An: _BJ-E-ID <E-ID@bj.admin.ch>
Betreff: AW: Einladung zur Konsultation "E-ID Technologie-Entscheid" / Invitation à la consultation "e-ID choix technologique"

Sehr geehrter Herr Rauschenbach

Besten Dank für die Möglichkeit zur Stellungnahme.
Unser Datenschutzbeauftragter und ich haben das Diskussionspapier besprochen.
Wir sind der Ansicht, dass es an ausreichenden Informationen fehlt um sich für ein Szenario entscheiden zu können. Szenario A erlaubt die Integration der E-ID in das europäische Umsystem. Zudem soll die eingesetzte Technologie erprobt sein. Im Umkehrschluss gibt es für Szenario B, das wohl datenschutzfreundlicher wäre (unlinkabilty bzw. reduzierte Trackingmöglichkeiten) wenig bis keine Informationen zur technischen Umsetzung, der Interoperabilität, der Akzeptanz einer anderen Technologie seitens der Europäischen Union (bspw. was fordert der Schengen-Besitzstand?) etc.. Insbesondere für Szenario B wären mehr Informationen erforderlich, um die Szenarien gegeneinander abwägen zu können.

Wir erlauben uns deshalb ihnen unsere Stellungnahme per E-Mail und nicht durch Ausfüllen des Antwortformulars zukommen zu lassen.

Freundliche Grüsse

Martin Jenny
Fachstellenleiter

kanton glarus - Staatskanzlei

Fachstelle Digitale Verwaltung
Rathaus, 8750 Glarus
Tel 055 646 60 04
www.gl.ch / staatskanzlei@gl.ch

Von: Plattner Roger (DJSG) <Roger.Plattner@djsg.gr.ch>
Gesendet: Donnerstag, 11. Januar 2024 08:19
An: _BJ-E-ID <E-ID@bj.admin.ch>
Betreff: Rückmeldung Konsultation "E-ID Technologie-Entscheid" / Invitation à la consultation "e-ID choix technologique"

Sehr geehrte Damen und Herren

Wir bedanken uns für die Gelegenheit zur Stellungnahme im obenstehenden Geschäft. Wir erachten den aktuellen Zeitpunkt als verfrüht, um zu beurteilen, welches der beiden Szenarien zu bevorzugen ist. Gerade auch vor dem Hintergrund, dass sich die Entwicklungen in der EU in diesem Bereich noch nicht abgeschlossen sind, ist uns insbesondere hinsichtlich des Szenario A eine abschliessende Bewertung nicht möglich. Wir haben daher auf eine Rückmeldung im Rahmen des Fragebogens verzichtet.

Beste Grüsse

Roger Plattner

Departement für Justiz, Sicherheit und Gesundheit Graubünden
Departement da giustia, segirezza e sanadad Grischun
Dipartimento di giustizia, sicurezza e sanità Grigioni
RA Dr. iur. Roger Plattner
Juristischer Mitarbeiter, Collavuratur giuridico, Collaboratore giuridico
Hofgraben 5, 7001 Chur
Tel.: +41 81 257 25 12
roger.plattner@djsg.gr.ch
www.djsg.gr.ch

Kanton St.Gallen
Sicherheits- und Justizdepartement

Oberer Graben 32, 9001 St.Gallen

Bundesamt für Justiz
Bundesrain 20
3003 Bern

Sicherheits- und Justizdepartement
Oberer Graben 32
9001 St.Gallen
T 058 229 36 00

St.Gallen, 15. Januar 2024

Konsultation "E-ID Technologie-Entscheid"

Sehr geehrter Herr Direktor

Mit E-Mail vom 1. Dezember 2023 wurden die Kantone zur Konsultation betreffend «E-ID Technologie-Entscheid» bis 3. Januar 2024 eingeladen. Diese Frist wurde schliesslich bis 15. Januar 2024 verlängert. Wir danken für diese Möglichkeit und nehmen gerne wie folgt in grundsätzlicher Hinsicht Stellung:

Aus unserer Sicht ist Szenario A klar zu bevorzugen. Es erscheint sinnvoll, eine international anschlussfähige Lösung anzustreben. Die Schweiz soll sich daher am Umsetzungsvorschlag der EU orientieren. Dabei unterstützen wir das im Bericht erwähnte schrittweise Vorgehen, wonach im Anschluss an die erfolgreiche Einführung das System parallel dazu auf weitere Technologien erweitert wird. Das Risiko, im Verlauf des Projekts Justierungen oder nach Abschluss der ersten Einführung Weiterentwicklungen vornehmen zu müssen, ist mit Blick auf die hohe Dringlichkeit, dass in der Schweiz in absehbarer Zeit eine «E-ID» eingeführt werden kann, hinzunehmen.

Freundliche Grüsse

SICHERHEITS- UND JUSTIZDEPARTEMENT
Der stellvertretende Vorsteher

Marc Mächler
Regierungsrat

Kopie per E-Mail an:
– rolf.rauschenbach@bj.admin.ch

Finanzdirektion, Postfach, 6301 Zug

Nur per E-Mail
Eidgenössisches Justiz- und Polizeidepartement EJPD
Herr Bundesrat Beat Jans
Bundeshaus West
3003 Bern

T direkt +41 41 728 36 01
heinz.taennler@zg.ch
Zug, 5. Januar 2024 hepa
FD FDS 6 / 282 / 138834

Konsultation «E-ID Technologie-Entscheid; Stellungnahme des Kantons Zug

Sehr geehrter Herr Bundesrat Jans
Sehr geehrte Damen und Herren

Mit E-Mail vom 1. Dezember 2023 hat das Eidgenössische Justiz- und Polizeidepartement (EJPD) den Kanton Zug eingeladen, zur Frage Stellung zu nehmen, mit welcher Technologie die E-ID Infrastruktur initial aufgebaut werden soll. Der Regierungsrat des Kantons Zug hat das Geschäft der Finanzdirektion zur direkten Beantwortung zugewiesen.

Kantonsintern haben wir einen Mitbericht der Sicherheitsdirektion, der Datenschutzstelle und des Amts für Informatik und Organisation eingeholt. Unsere Antworten zu den gestellten Fragen finden Sie im Word-Format in der Beilage. Ausserdem haben wir unsere Stellungnahme direkt in das zur Verfügung gestellte Online-Antwortformular (Findmind) eingetragen.

Für die Berücksichtigung unserer Anliegen danken wir Ihnen zum Voraus bestens.

Freundliche Grüsse
Finanzdirektion

Heinz Tännler
Regierungsrat

Beilage:
- Antwortformular (Findmind) im Word-Format

Versand per E-Mail an:

- E-ID@bj.admin.ch (Word- und PDF-Format)
- rolf.rauschenbach@bj.admin.ch
- Staatskanzlei (info.staatskanzlei@zg.ch, Geschäftskontrolle)
- Datenschutzstelle (datenschutz.zug@zg.ch)
- Sicherheitsdirektion (info.sd@zg.ch)
- Finanzdirektion (info.fd@zg.ch)
- Amt für Informatik und Organisation (info.aio@zg.ch)

Kanton Zug

Finanzdirektion
Direktionssekretariat

FD FDS 6 / 282 / 139351

Antwortformular (Findmind)

Discussion Papier: Initial technological basis for the Swiss national trust infrastructure

FD FDS 6 / 282 / 138925

Response form for the informal consultation about «Defining a common ground for the Swiss electronic identity and other verifiable credentials»

Instructions:

- Please fill out the form for your response.
- Feedbacks can be written in english, french, german oder italian.
- Please place open questions in the GitHub-Discussion Space.
- Consider that the current discussion does not need to cover the same topics mentioned in past public consultations (Zielbild E-ID, public consultation on the preliminary draft law).
- All responses will be published after the consultation period has expired, including indication of the official sender.

Which scenario would you prefer?

☒ Scenario A

☐ Scenario B

For what reason do you prefer that scenario?

Szenario A) verwendet je ein normiertes Protokoll für die Identität und das Ausstellen/Verifizieren. Dies ermöglicht bestmöglich die zukünftige Interoperabilität mit beispielsweise der EU. Als Nachteil zur Variante B) ist ein möglicher Verlust der Anonymität und Unverkettbarkeit durch den Verifier oder die Trust Registry möglich.

Szenario B) reduziert das Risiko des Verlusts zum Beispiel der Anonymität mittels proprietären Protokolls. Dafür entstehen höhere Risiken bei der Entwicklung und Implementation, weil Praxiserfahrungen teilweise noch fehlen.

Grundsätzlich ist darauf hinzuweisen, dass die Konsultation der Bundesverwaltung früh erfolgt ist, da der Gesetzgebungs- und Standardisierungsprozess in der EU noch nicht abgeschlossen ist und in der EU derzeit lediglich ein unverbindlicher Referenzrahmen einer Expertengruppe

Baarerstrasse 53, 6300 Zug
T +41 41 728 36 03
zg.ch/finanzen

für die technischen Spezifikationen der digitalen Identität vorliegt. Nicht abschliessend beurteilt werden kann daher, wie sich die in Kapitel 4.5 Unberücksichtigte Aspekte erwähnten Punkte wie zusätzliche Hardware/crypto-chip based wallet security auf die zwei Technologievarianten auswirken können. Klar ist jedoch, dass im Interesse der Wirtschaft und der Bürger eine international anschlussfähige Lösung im Vordergrund stehen muss und mit der Entwicklung nicht weiter zugewartet werden darf.

Um die Digitalisierung der Leistungen der öffentlichen Hand auf das nächste Level zu bringen, ist eine nationale E-ID dringend notwendig. Die Zeit und das Risiko des Scheiterns bei einem Alleingang sind deshalb wichtige Entscheidungsfaktoren. Es kann angenommen werden, dass die Weiterentwicklung der Architektur der EU den heute diskutierten Schwächen Rechnung tragen wird und die Schweiz an der von Anfang an EU-kompatiblen Lösung eigene Verbesserungen anstreben kann.

Als global denkende und handelnde Schweiz ist die Interoperabilität und Nutzung der E-ID mindestens mit den umliegenden Ländern unbedingt anzustreben. Durch die multinationale Nutzung im Onlinebereich ergeben sich neben Vorteilen wirtschaftlicher Natur vor allem persönliche Vorteile beim Reisen wie Hotel-Check-in, Altersprüfungen, etc.

Fazit: Szenario A) baut auf einer bekannten Technologie auf – deren Umsetzung bietet grösstmögliche Interoperabilität mit der EU.

Do both scenarios fulfil your expectations?

[Yes

[No

What major risks do you foresee?

Um als führendes digitales Land wahrgenommen zu werden, ist eine baldige E-ID Lösung unbedingt anzustreben. Das kann grundsätzlich mit beiden Varianten erreicht werden. Die Komplexitätsrisiken im Szenario B, kombiniert mit der kleineren Entwickler-Community könnten jedoch zu kostspieligen Verzögerungen führen.

Which «red lines» should not be crossed? Where is no compromise conceivable for you?

Die Herausgabe der schweizerischen E-ID darf wegen dem Technologie-Entscheid nicht verzögert werden. Es muss unbedingt verhindert werden, dass Besitzerinnen und Besitzer der CH-E-ID sich aufgrund eines Technologiewechsels nochmals registrieren müssen. Das würde die Glaubwürdigkeit an die E-ID massiv in Frage stellen (Imageverlust).

Da der Issuer und die Trust Registry im schweizerischen Fall staatlich sind, muss der Aspekt des möglichen Verlustes der Anonymität im Szenario A) durch staatliche Massnahmen auf ein tragbares Risiko reduziert werden.

Addition remarks

Wir erwarten, dass uns Konsultationen bzw. Vernehmlassungen künftig nicht mehr in englischer, sondern in deutscher Sprache und als Word-Datei zur Verfügung gestellt werden. Gemäss Art. 4 der Bundesverfassung der Schweizerischen Eidgenossenschaft sind unsere Landessprachen Deutsch, Französisch, Italienisch und Rätoromanisch und nicht Englisch. Dies gilt auch im Verkehr zwischen dem Bund und den Kantonen.

Ausserdem bitten wir Sie, für Konsultationen keine Online-Formulare zu verwenden, da uns Online-Umfragen, die nicht ausgedruckt werden können und die nicht als Word-Dateien zur Verfügung stehen, die Einholung von Mitberichten anderer Direktionen und der kantonalen Datenschutzstelle und die Antragstellung an den Regierungsrat des Kantons Zug verunmöglichen.

Schliesslich weisen wir Sie darauf hin, dass Artikel 7 des Bundesgesetzes vom 18. März 2005 über das Vernehmlassungsverfahren (Vernehmlassungsgesetz, VIG, SR 172.061) eine ordentliche Vernehmlassungsfrist von drei Monaten vorschreibt.

Davon abgesehen begrüssen wir das gewählte Vorgehen, Interessierte und Interessengruppen in einer breit angelegten Vernehmlassung zu dieser absoluten Schlüsseltechnologie zu konsultieren.

Official Sender

Finanzdirektion des Kantons Zug
Baarerstrasse 53
6300 Zug
info.fd@zg.ch

Kanton Zürich
Staatskanzlei

Dr. iur. Kathrin Arioli
Staatsschreiberin

Neumühlequai 10
8090 Zürich
Telefon +41 43 259 20 93
franziska.moser@sk.zh.ch
www.zh.ch

Eidgenössisches Justiz- und Polizeidepartement
Bundesamt für Justiz
Dr. rer. publ. Rolf Rauschenbach
Informationsbeauftragter E-ID
Bundesrain 20
3003 Bern

15. Januar 2024
Konsultation "E-ID Technologie-Entscheid"

Sehr geehrter Herr Rauschenbach

Wir danken Ihnen für die Einladung zur Konsultation zum E-ID-Technologie-Entscheid vom 1. Dezember 2023 und die gewährte Fristverlängerung bis 22. Januar 2024.

Das Projekt E-ID und die Entwicklungen auf rechtlicher Ebene sind für den Kanton Zürich von höchster Wichtigkeit. Wir begrüssen es deshalb, im Rahmen dieser Konsultation Stellung nehmen zu können. Um fristgerecht eine rechtspolitisch fundierte Rückmeldung geben zu können, haben wir das EuropaInstitut an der Universität Zürich mit einer Stellungnahme beauftragt.

Die Stellungnahme weist im Ergebnis darauf hin, dass die Entwicklungen in der EU einerseits mit Bezug auf die technische Umsetzung der digitalen Identität und der hierbei verwendeten Spezifikationen sowie anderseits betreffend die Datenschutzstandards bei der hierbei auftretenden Verarbeitung personenbezogener Daten noch nicht abgeschlossen sei. Eine abschliessende Beantwortung der aufgeworfenen Fragen sei deshalb derzeit kaum möglich. Unter Einbezug möglicher weiterer Entwicklungen sollte jedoch eine international anschlussfähige Lösung im Interesse der Wirtschaft und der Bevölkerung im Vordergrund stehen.
Dieser Schlussfolgerung können wir uns vollumfänglich anschliessen. Gerne lassen wir Ihnen die Stellungnahme des EuropaInstituts anbei zur Kenntnisnahme zukommen.

Wir danken Ihnen für die Berücksichtigung dieser Rückmeldung.

Freundliche Grüsse

Dr. iur. Kathrin Arioli

Beilagen
– Rechtspolitische Stellungnahme des Europainstituts der Universität Zürich

EuropaInstitut
AN DER UNIVERSITÄT ZÜRICH

Diskussionspapier der Bundesverwaltung vom 12. Dezember 2023: Erste technologische Umsetzung für die Schweizer Vertrauensinfrastruktur – Festlegen einer gemeinsamen Grundlage für die elektronische Identität der Schweiz und andere elektronische Nachweise

Rechtspolitische Stellungnahme

1. Auftrag und Vorgehen

Die Staatskanzlei des Kantons Zürich hat das Europa Institut an der Universität Zürich am 14. Dezember 2023 mit einer rechtspolitischen Stellungnahme zur Konsultation der Bundesverwaltung vom Dezember 2023 zur elektronischen Identität in der Schweiz befasst. Gegenstand der Konsultation ist die Frage, ob sich die Schweiz bei der Einführung einer elektronischen Identität an die technischen Spezifikationen der EU anlehnen (Szenario 1) oder eigenständige technische Standards verfolgen sollte (Szenario 2). Massgebliche Pole bei der Entscheidungsfindung sind laut den Konsultations-unterlagen einerseits die internationale Kompatibilität bzw. Einsetzbarkeit der digitalen Identität und andererseits der Schutz persönlicher Daten der Schweizer Bürger.

Bei der Beurteilung der in den Konsultationsunterlagen aufgeworfenen Fragen sind in rechtspolitischer Hinsicht verschiedene Überlegungen anzustellen:

- Standardisierungsprozess:

Bei der Entscheidung für oder gegen eine Übernahme von EU-Standards ist zunächst bedeutsam, ob die betreffenden technischen Spezifikationen bereits klar genug und verbindlich festgelegt wurden oder ob der Ausgang des Standardisierungsprozesses in der EU noch offen und nicht vollständig absehbar ist.

- Datenschutzrechtliche Implikationen:

Weiterhin ist bei der Entscheidung für eines der in den Konsultationsunterlagen aufgeworfenen Szenarien bedeutsam, welche datenschutzrechtlichen Standards die EU bei der Umsetzung Implementierung der digitalen Identität zugrunde legt und ob diese den Schweizer Anforderungen an den Datenschutz genügen.

- Zeitliche Dimension bei der Entscheidungsfindung:

Die voranstehenden Überlegungen führen zu der Frage, zu welchem Zeitpunkt die Schweiz sinnvollerweise über eine Anlehnung an bzw. Übernahme von EU-Standards bei der Implementierung einer digitalen Identität entscheiden sollte und ob die vorliegende Konsultation zu früh erfolgt.

2. Standardisierungsprozess

Bei der Entscheidung für oder gegen eine Übernahme von EU-Standards ist zunächst bedeutsam, ob die technischen Lösungsansätze und Spezifikationen der EU, auf welche das Konsultationspapier verweist, bereits klar genug und verbindlich festgelegt wurden oder ob der Ausgang des Standardisierungsprozesses in der EU noch offen und nicht vollständig absehbar ist.

Hintergrund

In der Europäischen Union wurde bereits im Jahr 2014 per Verordnung ein Rechtsrahmen für die Schaffung einer europäischen digitalen Identität verabschiedet.[1] Eine Bewertung dieser Verordnung ergab, dass sie den technologischen Innovationen der letzten Jahre sowie neuen Marktanforderungen nicht mehr gerecht werde; vor diesem Hintergrund legte die Europäische Kommission am 3. Juni 2021 einen Vorschlag zur Revision dieser Verordnung vor.[2] Kernbereiche des Revisionsvorschlags sind die Förderung der Kohärenz bei der Nutzung elektronischer Vertrauensdienste[3], die Ausweitung des Anwendungsbereichs auf zusätzliche Vertrauensdienste (u.a. elektronische Signaturen und Siegel) sowie die Einführung einer digitalen Brieftasche.[4]

Stand der Revision

Der gegenständliche Vorschlag zur Revision der Verordnung von 2014 wurde bislang noch nicht verabschiedet. Nach aktuellem Verfahrensstand[5] hat die Kommission den Vorschlag an den Rat weitergeleitet, der zwischen Juni und Dezember 2023 bereits mehrere Erörterungen durchgeführt hat. Das Europäische Parlament hat sich indes bislang noch nicht mit dem Rechtsakt befasst. Als Co-Gesetzgeber müssen sich der Rat und das Parlament in bis zu drei Lesungen auf eine Textfassung einigen, bevor der Rechtsakt dann von den Präsidenten beider Institutionen unterzeichnet und per Veröffentlichung im Amtsblatt in Kraft gesetzt wird.

---

[1] Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, ABl. L 257 vom 28.8.2014, S. 73.

[2] Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität, COM(2021) 281 final vom 3. Juni 2021, S.1.

[3] Ein Vertrauensdienst ist gemäss Definition des Verordnungsvorschlags ein elektronischer Dienst, der in der Regel gegen Entgelt erbracht wird und aus Folgendem besteht: Erstellung, Überprüfung und Validierung von elektronischen Signaturen, Siegeln oder elektronischen Zeitstempeln etc., vgl. COM(2021) 281, S. 25.

[4] Bei der elektronischen Brieftasche handelt es sich gemäss der Definition des Verordnungsvorschlags um ein Produkt bzw. Dienst, das bzw. der es dem Nutzer ermöglicht, mit seiner Identität verknüpfte Identitätsdaten, Berechtigungsnachweise und Attribute zu speichern, vertrauenden Beteiligten auf Anfrage vorzuweisen und sich damit online und offline bei einem Dienst zu authentifizieren sowie qualifizierte elektronische Signaturen oder Siegel zu erstellen, vgl. COM(2021) 281, S. 26

[5] 21. Dezember 2023.

Unklar bzw. missverständlich ist insoweit eine Pressemitteilung der Europäischen Kommission vom 8. November 2023, in welcher sie verkündete, dass sich der Rat und das Parlament über die gegenständliche Revisionsverordnung «endgültig geeinigt» haben.[6] Wie den Unterzeichnern auf telefonische Rückfrage bei der Europäischen Kommission bestätigt wurde, haben bislang allein 4 sogenannte «Trilog-Verhandlungen» stattgefunden; das ordentliche Gesetzgebungsverfahren wurde noch nicht abgeschlossen.[7] Hierbei handelt es sich um informelle Verhandlungen zwischen Vertretern des Rates, des Europäischen Parlaments und der Europäischen Kommission, bei denen Vorsondierungen und Kompromisslösungen verfolgt werden. Entsprechende Vorverhandlungen sind in den Bestimmungen zum Rechtssetzungsverfahren in den Gründungsverträgen der EU nicht vorgesehen.[8] Hervorzuheben ist hierbei, dass die nach ordentlichen Gesetzgebungsverfahren vorgesehenen Verhandlungen im Parlament öffentlich stattfinden, während die informellen Trilog-Verhandlungen üblicherweise unter Ausschluss der Öffentlichkeit durchgeführt werden, womit die Einflussnahme durch externe Interessengruppen erschwert wird. Bezogen auf den gegenständlichen Verordnungsvorschlag bedeutet dies, dass wohl bereits ein gewisser Konsens zwischen Rat, Parlament sowie Kommission gefunden wurde. Dieser Konsens ist indes informeller Natur. Juristisch entscheidend ist die erst noch stattfindende Lesung im Parlament, innerhalb welcher noch Änderungsanträge ergehen können; in diesem Falle müsste anschliessend der Rat noch etwaigen Änderungsanträgen zustimmen, bevor der Rechtsakt verabschiedet werden kann.

Laut telefonischer Auskunft der Europäischen Kommission wird damit gerechnet, dass die Lesung im Parlament voraussichtlich im Februar 2024 stattfindet und anschliessend zeitnah die Verordnung erlassen wird. Die letzte verfügbare Fassung des mehrfach geänderten Vorschlagstextes datiert auf den 10. November 2023 und dokumentiert den Diskussionsstand der zuvor durchgeführten Trilog-Verhandlungen.[9] Ein definitiver und verbindlicher Verordnungstext, an dem sich die Schweiz orientieren könnte, existiert gegenwärtig noch nicht.

Festlegung technischer Stand

Auch wenn der finale Text der in Revision befindlichen Verordnung noch nicht vorliegt, zeichnet sich bereits ab, dass die konkreten technischen Spezifikationen zur Umsetzung der digitalen Identität bzw. Brieftasche nicht in der Verordnung selbst geregelt werden. Die vorgeschlagene Revisionsverordnung umfasst vielmehr eine Bestimmung, mit welcher der Rat und das Parlament die Europäischen Kommission ermächtigen und verpflichten, innerhalb von 6 Monaten nach Inkrafttreten der Verordnung die technischen Spezifikationen und Bezugsnormen für die elektronische Identität und Brieftasche im

---

[6] Pressemitteilung der Europäischen Kommission, IP/23/5651 vom 8. November 2023 («Kommission begrüsst endgültige Einigung über EUid-Brieftasche»); abrufbar unter: https://ec.europa.eu/commission/presscorner/detail/de/ip_23_5651.

[7] Europäische Kommission, Generaldirektion Kommunikationsnetze, Abteilung eID Technical Framework, Abteilungsleiter Norbert Sagstetter, +352 4301 35460, Telefonat vom 18. Dezember 2023.

[8] Lediglich eine Gemeinsame Erklärung des Europäischen Parlaments, des Rats und der Kommission vom 30. Juni 2023 statuiert «praktische Modalitäten des neuen Mitentscheidungsverfahrens (Art. 251 EG-Vertrag)», wobei auf das Phänomen der «Triloge» Bezug genommen wird. Diese Erklärung dürfte indes keine hinreichende Grundlage für eine Änderung bzw. Ergänzung des in den Gründungsverträgen festgelegten Gesetzgebungsverfahrens bilden; ABl. C 145 vom 30. Juni 2007, S. 5.

[9] https://data.consilium.europa.eu/doc/document/ST-15149-2023-INIT/en/pdf.

Wege eines Durchführungsrechtsakts zu festzulegen.[10] Im Rahmen des ordentlichen Gesetzgebungsverfahrens in der EU figurieren zwar ausschliesslich das Europäische Parlament und der Rat als Ko-Gesetzgeber. Im Falle der Reglementierung technischer Detailfragen, die in Abhängigkeit der Entwicklung des Umfelds in spezifischen Sektoren zeitnah revidiert werden müssen, können das Europäische Parlament und der Rat per Verordnung oder Richtlinie der Europäischen Kommission inhaltlich und temporär begrenzte Kompetenzen zum Erlass solcher Durchführungsrechtsakte einräumen.[11] Erlässt die Europäische Kommission eine entsprechende Durchführungsverordnung, entfaltet diese rechtsverbindliche Wirkung gegenüber den Mitgliedstaaten.

In Vorbereitung einer entsprechenden Durchführungsverordnung mit technischen Details hat die Europäische Kommission zeitgleich mit der Veröffentlichung des gegenständlichen Verordnungsvorschlags eine Empfehlung veröffentlicht, in der sie den Mitgliedstaaten rät, ein gemeinsames Instrumentarium für ein koordiniertes Herangehen an einen Rahmen für die europäische digitale Identität zu entwickeln.[12] In Reaktion auf diese Empfehlung hat eine von den EU-Mitgliedstaaten einberufene Expertengruppe[13] ein entsprechendes Referenzdokument mit technischen Spezifikationen zur digitalen Identität und zur digitalen Brieftasche erarbeitet.[14] In den einleitenden Kapiteln dieses Dokuments wird ausdrücklich darauf hingewiesen, dass der enthaltene technische Referenzrahmen keine rechtliche Wirkung entfaltet und auch nicht den noch anstehenden Rechtsetzungsaktivitäten vorweggreifen. Lediglich die Revisionsverordnung und die auf ihrer Grundlage erlassenen Durchführungsrechtsakte seien für die Mitgliedstaaten verbindlich.[15] Der Zweck des Dokuments läge insbesondere in der Bereitstellung eines Referenzrahmens für laufende Pilotprojekte zur digitalen Brieftasche. Erfahrungen, welche in diesem Rahmen gewonnen würden, könnten in aktualisierte Versionen des Referenzrahmens einfliessen. Gemäss diesem Hinweis wurde das Referenzdokument in der Zwischenzeit bereits mehrfach aktualisiert.

Laut telefonischer Auskunft der Europäischen Kommission ist mit einer neuen Fassung des Referenzrahmens im Jahr 2024 zu rechnen, und zwar zeitnah zu der für die erste Jahreshälfte prognostizierten offiziellen Verabschiedung der Revisionsverordnung.[16] Inwieweit die technischen Spezifikationen in dem aufdatierten Referenzrahmen dann tatsächlich in eine Durchführungsverordnung übernommen werden und dadurch verbindlich werden, sei noch nicht vollends absehbar.

Abschliessend ist festzuhalten, dass sich das Konsultationsdokument der Bundesverwaltung in seinem Szenario A auf vermeintliche EU-Spezifikationen bezieht, die zum

---

[10] Art. 6a Ziff. 11 COM(2021) 281, S. 29.

[11] Art. 290, 291 Vertrag über die Arbeitsweise der Europäischen Union (AEUV).

[12] Empfehlung (EU) 2021/946 der Kommission vom 3. Juni 2021 für ein gemeinsames Instrumentarium der Union für ein koordiniertes Herangehen an einen Rahmen für die europäische digitale Identität, ABl. L 210 vom 14. Juni 2021, S. 51.

[13] eIDAS Expert Group; vgl. https://ec.europa.eu/transparency/expert-groups-register/screen/expert-groups/consult?lang=en&groupID=3032.

[14] The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework – The European Digital Identity Wallet Architecture and Reference Framework (ARF); abrufbar unter: https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-wallet-architecture-and-reference-framework.

[15] Vgl. ARF, S. 5.

[16] Europäische Kommission, Generaldirektion Kommunikationsnetze, Abteilung eID Technical Framework, Abteilungsleiter Norbert Sagstetter, +352 4301 35460, Telefonat vom 18. Dezember 2023.

gegenwärtigen Zeitpunkt lediglich in einem unverbindlichen Expertendokument aufgeführt werden; dieses Dokument wurde bereits mehrfach aufdatiert und soll im Frühjahr 2024 ein weiteres Mal aktualisiert werden. Ob, wann und welche Spezifikationen in der EU verbindlich werden, ist zum gegenwärtigen Zeitpunkt nicht absehbar. Erst innerhalb von 6 Monate nach der offiziellen Annahme der Revisionsverordnung muss die Europäische Kommission in einer Durchführungsverordnung die technischen Spezifikationen verbindlich festlegen. Frühestens in der zweiten Jahreshälfte 2024 dürfte hiermit zu rechnen sein. Zum gegenwärtigen Zeitpunkt hat das Szenario A bei näherer Betrachtung somit wenig klare Konturen. Es handelt sich eher um eine Marschrichtung der EU mit unklarem Ausgang. Die genauen technischen Spezifikationen und deren Verbindlichkeit werden wohl erst gegen Ende 2024 näher definiert sein.

3. Datenschutzrechtliche Implikationen

Weiterhin ist bei der Entscheidung für eines der in dem Konsultationsdokument aufgeworfenen Szenarien bedeutsam, welche datenschutzrechtlichen Standards die EU bei der Implementierung der digitalen Identität zugrunde legt. Soweit ersichtlich waren insbesondere auch datenschutztechnische Aspekte der Grund dafür, ein Szenario B mit einer eigenständigen technologischen Lösung für die Schweiz zu erarbeiten.

Zunächst ist festzuhalten, dass dem Datenschutz in der Europäischen Union ein grosser Stellenwert beigemessen wird. Prominent kommt dies bereits in der EU-Grundrechtscharta zum Ausdruck, deren Art. 8 dem Recht auf Schutz personenbezogener Daten den Rang eines Grundrechts beimisst.[17] Mit der Aufnahme dieses Rechts in die Grundrechtscharta werden die EU und ihre Organe bei der Annahme von Sekundärrecht sowie bei der Rechtsprechung umfassend gebunden, wie auch die Mitgliedstaaten bei der Anwendung des einschlägigen EU-Rechts. Einschränkungen des Rechts auf den Schutz personenbezogener Daten sind nur unter den engen Voraussetzungen des Art. 52 der EU-Grundrechtscharta zulässig[18].

Darüber hinaus hat die EU mit der Datenschutz-Grundverordnung[19] und der Richtlinie für den Datenschutz in den Bereichen Polizei und Justiz[20] von 2016 die wohl weltweit strengsten Zulässigkeitsanforderungen an die Verarbeitung personenbezogener Daten erlassen. Die Vorschriften besitzen extraterritoriale Wirkung für Akteure ausserhalb der EU, soweit sie Dienstleistungen auf dem Binnenmarkt der EU anbieten und hierbei Daten von EU-Bürgern verarbeiten. Zentrale Bereiche der EU-Datenschutz-Grundverordnung wurden zudem anlässlich der jüngsten Datenschutzrechtsrevision von der Schweiz übernommen. Von daher ist grundsätzlich von einem hohen Datenschutzniveau in der EU

[17] Charta der Grundrechte der Europäischen Union, ABl. C 364 vom 18. Dezember 2000, S. 1.

[18] Hiernach sind Einschränkungen zulässig, wenn sie gesetzlich vorgeschrieben sind, den Wesensgehalt des Rechts auf Datenschutz achten und unter Wahrung des Grundsatzes der Verhältnismässigkeit erforderlich sind.

[19] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Text von Bedeutung für den EWR), ABl. L 119 vom 4. Mai 2016, S. 1

[20] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. L 119 vom 4. Mai 2016, S. 89.

auszugehen, welches dem Datenschutzniveau in der Schweiz zumindest regulatorisch entspricht.

Im Hinblick auf die vorgeschlagene technische Umsetzung einer digitalen Identität in der EU wurden von Seiten der Wissenschaft und Praxis verschiedene datenschutzrechtliche Bedenken angemeldet. Hervorzuheben ist insoweit ein offener Brief von 500 Wissenschaftlern und NGOs vom 9. November 2023.[21] Die Kritik bezieht sich einerseits auf technische Lösungen im Entwurf der Revisionsverordnung (Art. 45), weiterhin auf bestimmte technische Spezifikation, die in dem unverbindlichen Referenzdokument der eIDAS-Expertengruppe aufgeführt werden sowie schliesslich auf das Problem der «Unlinkability», welches auch in den gegenständlichen Konsultationsunterlagen der Bundesverwaltung erwähnt wird.[22]

Diesbezüglich ist festzustellen, dass der erste Entwurf der Revisionsverordnung vom 3. Juni 2021 tatsächlich lediglich in den Erwägungsgründen darauf hinwies, dass die Verarbeitung von personenbezogenen Daten beim Einsatz der digitalen Identität «in Einklang mit der Datenschutz-Grundverordnung erfolgen sollte».[23] Vergleicht man diesen ursprünglichen Text des Kommissionsvorschlags mit der Kompromissfassung nach der letzten Trilog-Verhandlung vom 8. November 2023[24], fällt auf, dass der Einhaltung datenschutzrechtlicher Belange an diversen Punkten in den Erwägungsgründen sowie auch im Verordnungstext selbst unterdessen Rechnung getragen wurde. So wurde etwa neu ein Recht auf Datenlöschung aus der digitalen Brieftasche ergänzt[25]. Auch thematisiert die aktualisierte Vorschlagsfassung explizit das Problem der «Unlinkability».[26] Ob es sich um die letzten Änderungen handelt und in welcher Fassung das Europäische Parlament in seiner noch ausstehenden ersten Lesung dem Verordnungstext zustimmen wird, lässt sich gegenwärtig noch nicht absehen. Es besteht aber zumindest der Eindruck, dass das Konsultationsdokument der Bundesverwaltung allenfalls zu einem früheren Zeitpunkt verfasst wurde und etwas verfrüht von bereits gesetzten und allenfalls nicht ausreichenden Datenschutzstandards in der EU ausgeht. Grundsätzlich sollte davon ausgegangen werden dürfen, dass die EU ihre eigenen Datenschutzbestimmungen einhält. Es sollte daher zunächst die finale Version der Revisionsverordnung abgewartet und geprüft werden, ob sie allfällige Ausnahmen oder einen Vorrang der Revisionsverordnung vor der DSGVO statuiert oder aber sogar – wie in der letzten Vorschlagsfassung – Datenschutzbelange explizit sicherstellt.

---

[21] https://www.patrick-breyer.de/eu-verordnung-ueber-digitale-identitaeten-eidas-piraten-unterstuetzen-keinen-blankoscheck-zur-online-ueberwachung-der-buergerinnen/.

[22] Diskussionspapier, S. 6.

[23] Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität, COM(2021) 281 final vom 3. Juni 2021, S.3.

[24] Rat der EU, Doc. 2021/0136(COD) vom 10. November 2023, abrufbar unter: https://data.consilium.europa.eu/doc/document/ST-15149-2023-INIT/en/pdf.

[25] Vgl. Art. 6a Ziff. 3 a (ii).

[26] Vgl. Art 6a Ziff. 7 b (b).

4. Zeitliche Dimension bei der Entscheidungsfindung

Die Konsultationsfrist der Bundesverwaltung zum Diskussionspapier über die Umsetzung der digitalen Identität wurde auf Anfang Januar 2024 gesetzt und liegt damit zeitlich Mitten in dem noch andauernden Gesetzgebungs- und Standardisierungsprozess in der EU. Es erfolgten bislang lediglich informelle Trilog-Verhandlungen zu dem Revisionsverordnungsvorschlag der Kommission vom Juni 2021, im Rahmen welcher umfangreiche Änderungen an der ursprünglichen Textfassung vorgenommen wurden. Diese betreffen sowohl technische Aspekte sowie auch datenschutzrechtliche Fragen. Wie das Europäische Parlament in seiner noch ausstehenden ersten Lesung über den Vorschlag befinden wird, ist noch offen.

Gleichermassen unklar sind auch die in der EU zum Einsatz kommenden technischen Spezifikationen bei der Umsetzung der digitalen Identität. Gegenwärtig existiert lediglich ein unverbindlicher Referenzrahmen einer Expertengruppe; dieser wird beständig aufdatiert und erhält Anfang nächsten Jahres eine weitere neue Fassung. Welche dieser Standards in eine verbindliche Durchführungsverordnung der Europäischen Kommission übernommen werden, lässt sich gegenwärtig noch nicht absehen. Sobald die Revisionsverordnung offiziell verabschiedet wurde, muss die Kommission innerhalb von 6 Monaten eine entsprechende Durchführungsverordnung erlassen. Hiermit ist wohl frühestens in der zweiten Hälfte 2024 zu rechnen.

5. Ergebnis

Im Ergebnis ist festzustellen, dass die Konsultation der Bundesverwaltung zu einem verfrühten Zeitpunkt erfolgt. Die Entwicklungen in der EU sind in massgeblichen Bereichen noch nicht abgeschlossen. Dies betrifft einerseits die technische Umsetzung der digitalen Identität und der hierbei verwendeten Spezifikationen sowie andererseits die Datenschutzstandards bei der hierbei auftretenden Verarbeitung personenbezogener Daten.

Der in den Konsultationsunterlagen im «Szenario A» bezeichnete Ansatz der EU ist tatsächlich nur ein Zwischenstadium in einem noch nicht abgeschlossenen, offenen Prozess. Eine abschliessende Beantwortung der aufgeworfenen Fragen ist daher kaum möglich. Vielmehr kann nur eventualiter, unter Einbezug möglicher weiterer Entwicklungen Stellung bezogen werden.

Grundsätzlich sollte eine international anschlussfähige Lösung bei der Einführung einer digitalen Identität im Interesse der Wirtschaft sowie auch im Interesse der Bürger im Vordergrund stehen. Wirtschafts- und Privatleben reichen heute über die Landesgrenzen hinaus; praktikable Identitätsnachweise spielen hierbei eine zentrale Rolle, wie sich nicht zuletzt auch in der Covid-Krise bei der grenzüberschreitenden Vorlage und Anerkennung von Impfzertifikaten gezeigt hat. Hiervon sollte nur abgewichen werden, wenn die EU tatsächlich von ihren eigenen, in der Datenschutz-Grundverordnung statuierten hohen Datenschutzstandards abweichen sollte. Dies müsste auf der Grundlage der finalen Version der gegenständlichen Revisionsverordnung sowie auf der Grundlage der in einer noch ausstehenden Durchführungsverordnung vorgegebenen technischen Spezifikationen geprüft werden. Ferner soll nicht unerwähnt bleiben, dass die Vereinheitlichung der digitalen Identitätsnachweise in grösserem Kontext steht; so beabsichtigt die EU die Effizienz der öffentlichen Dienste durch eine breiter angelegte Zusammenarbeit zwischen

den nationalen Verwaltungen zu verbessern[27] und allgemein die Interoperabilität des öffentlichen Sektors in der Union zu fördern[28].

Es steht nun im Ermessen der Auftraggeberin, allenfalls auf einen späteren Zeitpunkt für die Durchführung der Konsultation hinzuwirken.

Zürich, 21. Dezember 2023

Dr. Tobias Baumgartner
Stv. Direktor

Prof. Dr. Andreas Kellerhals
Direktor

[27] Mitteilung der Europäischen Kommission, Enhancing the European Admimistrative Space (ComPAct), COM(2023) 667 vom 25. Oktober 2023.

[28] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Massnahmen für ein hohes Mass an Interoperabilität des öffentlichen Sektors in der Union, COM(2022) 720 vom 18. November 2022.

DIDAS Statement for E-ID Technology
Discussion Paper

Submitted and published to:
E-ID Team & via www.DIDAS.swiss blogpost

Submitted by:
Digital Identity and Data Sovereignty Association (www.didas.swiss)
Campus Zug Rotkreuz
Surstoffi 1
CH-6343 Rotkreuz
info@didas.swiss

Dear E-ID Team, dear Ladies and Gentlemen

As a continuation of our form-submitted statement on the discussion paper for the «Initial technological basis for the Swiss trust infrastructure», we would like to thank you for the opportunity to comment in an extended format.

The «Digital Identity and Data Sovereignty Association» (DIDAS) is a Swiss non-profit association that was founded with the aim of «Establishing and promoting Switzerland as a leading ecosystem in the development and implementation of privacy-enhancing technologies, services and products that preserve and apply digital identity and electronically verifiable data».

We appreciate the Federal Administration's open approach and the high quality of the draft legislation as well as the technology discussion document. In addition, the understanding and application of a principle-based, iterative, and collaborative approach as critical success factors for the planning and implementation of a sustainable trust infrastructure, the establishment of an electronic identity and other digital proofs, as well as their widespread adoption and use, must be acknowledged.

We are very pleased that DIDAS and its members have been able to make a valuable contribution to the clarification process. This statement is a joint effort by all members of the DIDAS association under the leadership of the executive board. However, to illustrate the weight of DIDAS, we are pleased to explicitly name some of the contributing individuals below (in alphabetical order):

- Michael Doujak, DIDAS, working group technology; Ergon Informatik AG, Product Manager
- Marco Dütsch, DIDAS, working group technology; IKEA, Lead AI Innovation Lab
- Pascal Gottret, DIDAS, working group lead supply chain; Meraxis Group, Head SAP Application Management
- Georg Grewe, Vereign AG, CEO
- Dr. Peter Janes, DIDAS, working group lead health; Abdagon AG, Founder and CEO
- Dr. André Kudra, ESATUS Schweiz AG, CIO
- This Loepfe, DIDAS, working group lead technology a.i.; Verein cardossier, CTO
- Daniel Saeuberli, DIDAS, president; Accelerate GmbH, Founder and Managing Partner
- Vasily Suvorov, DIDAS, board member, working group technology; movos, CTO
- Kai Wagner, DIDAS, working group lead public sector; Procivis AG, Head of Products and Partners
- Prof. Dr. Tim Weingärtner, Lucerne University of Applied Sciences and Arts HSLU

- Richard F. Zbinden, DIDAS, working group technology; Rigiblue®, Founder and CEO

We continue to proudly advocate for SSI principles, as an important north star on this journey.

Rotkreuz, February 2024

Daniel Säuberli President	Tim Weingärtner Vice President	Diego Benz Board Member
Marco Dütsch Board Member	Ursula Sury Board Member	Vasily Suvorov Board Member

Additional Considerations to the Feedback on the Technology Discussion Paper

The goal of the «Discussion Paper: Initial technological basis for the Swiss trust infrastructure» is to determine the basic technology of the future trust infrastructure the E-ID will be issued to. The paper limits itself to the credential format and the protocols required to exchange such credentials.

While this focus on the very basis of the technology stack allows for a more targeted discussion and decision, it also loses some of the relevant aspects that determine if the technology is fit for purpose.

In our discussions at DIDAS, we have come up with an approach that considers the purpose for which the E-ID and other verifiable credentials are intended to be used. In the following additional considerations, we outline why we believe that such an approach is viable and should be considered as the technology stack of Switzerland's trust infrastructure.

In addition to the technological aspects of our official response, this document aims to convey important considerations to a wider, less technological target audience.

No pure scenario A or B decision possible

After intensive discussions within and across the working groups, it became clear that both scenarios have technological shortcomings, such that the requirements for the E-ID in accordance with paragraph 2.1 of the technology discussion paper cannot be fully met.

As a result, we have come to realize that a simple decision in favor of one of the proposed scenarios is not enough and therefore cannot be supported.

Whenever a decision cannot lead to a viable solution, the framework conditions may need to be challenged or the proposals must be extended accordingly. This is what we did at DIDAS and tried to enrich the two scenarios technologically to make a clear statement within the framework or to formulate a target-oriented recommendation. In this respect, in addition to answering the questions, we have also drawn up this additional statement. The officially form-submitted response with our «A+» recommendation can be found in the appendix.

The need to act now

It is important to note that, even with the proposed measures, scenario A+ is still far from ideal. The concerns around over-identification, linkability of credentials usage leading to correlation of identity and potential profiling, are hard to avoid completely with the currently available technologies and respective trade-offs. At the same time, the introduction of reusable electronic identity tools and their usage in corresponding systems is accelerating globally and it is, therefore, better to lead and establish a basis of a sovereign infrastructure, before other solutions take root, that might not be closely aligned with our Swiss values.

Scenario A+ is aligned with the direction that EU is taking and represents a reasonable compromise, which will allow us to gain valuable, first-hand experience with real use-case, understand limitations of the current and properly evaluate emerging technologies.

It is, consequently, an integral part of this proposal that A+ is seen as an intermediate **starting point** that allows for iterative, continuous further development and improvement of the technological infrastructure. We expect that the suggestion described in the section «Opportunity Switzerland» will be viewed as the unalienable part of our proposal moving forward.

Current state of technology – what is possible, what isn't?

A key requisite for qualified digital identities is cryptographically safe owner binding. Technically, this requires cryptographic primitives «in silicon» in secure elements of devices (typically mobile phones) to prevent any type of misuse or owner faking.

Specifically, the private / public key pair must be generated «in silicon» of the secure element of the device, and the private key must never leave the secure element to prevent any case of misuse by copying the private key. Such technology is a mandatory prerequisite for qualified credentials and thus the E-ID (this was also the case for prior implementations with the same level of trust).

This technology is available for scenario A, but presently not supporting scenario B. Based on current research, hardware support for BBS+ curves, as suggested in scenario B, is not expected to be available within the next five years, due to technology uncertainties as well as the weaker community effort behind it.

Ways to be ready by 2026

Although (unfortunately) not explicitly stated in the draft of the E-ID act (BGEID), certain relevant use cases, such as registering for the national electronic health record (EPD) or legally binding digital signatures, require qualified digital identities based on current law.

This implies that qualified digital identities and hence credentials are a mandatory requirement for the E-ID, scheduled to be available by 2026. Consequently, this requirement rules out scenario B for qualified credentials until 2026 because cryptographic libraries in software for BBS+ are insufficient for qualified credentials.

While we recommend to closely monitor developments in this area for safe alternatives, this leaves us with scenario A for qualified credentials.

To avoid criticism of opponents in the political process, mitigating measures must be taken to address known weaknesses of the technology as much as possible, hence we converged on scenario A+. Specifically:

- To enforce this approach, only certified wallets shall be permitted to receive a qualified E-ID. Such certified wallets ensure that only authorized verifiers can obtain a qualified E-ID and potentially also limit the set of claims an authorized verifier may request.
- Ephemeral credentials – to allow the private sector to benefit from the new E-ID, we propose to complement the qualified E-ID with a number (e.g. 100) substantial and less restrictive E-IDs.

With these measures in place, the shortcomings of scenario A will be mostly addressed, and both government and private sector use cases can benefit from identities provided by the most trustworthy source for identity information.

Implementing both scenarios, A and B in parallel for the coming two years (as has been discussed internally) would incur substantial complexity for all issuers and verifiers. This would increase the project risk and it would endanger the envisioned availability by 2026.

It is our recommendation to focus on scenario **A+ with its proven technology as initial technology basis for Switzerland's E-ID trust infrastructure**, and we are putting emphasis on key extensions to consider in the financing package of the project.

Further, to cater for technology developments in this fast-moving field, the trust infrastructure **must be designed with its evolution in mind, right from day one.** It is to be designed based on a modular architecture and technology stack as well as multi-protocol support, so the platform can be continuously improved and expanded to other relevant technologies such as mDL, JSON-LD, BBS+, etc. as per the general technological availability and adaptability, as well

as key societal, public, and private stakeholders' needs. We recommend establishing a governance body as part of a wider framework, to help guide this evolution.

Coexistence of Qualified and Substantial Credentials

The **qualified E-ID** is applicable for a limited number of use cases where a high level of trust is required. The qualified E-ID shall be limited to specifically authorized and trusted verifiers, limiting over-identification. The heightened privacy requirements incur explicit user confirmation of every proof request, reducing user experience and convenience to some extent.

Each **substantial E-ID** (of the ephemeral certificates) is intended to be used in only one context to prevent linkability across verifiers, fully transparent to users. Substantial E-IDs shall also have some claims removed (e.g. AVS13) to again reduce the risk of privacy issues.

A less restrictive substantial E-ID is sufficient for most private sector use cases. It allows private keys to be stored without the need of secure elements on devices and cryptographic primitives «in silicon», and therefore offers more convenient solutions for use cases like automating proof requests based on personal preferences and policies, migrating to a new device, or using multiple devices in parallel. In all other aspects (e.g. cryptographic algorithms, credential formats) the substantial E-ID uses the same technology as the qualified E-ID and therefore simplifies the implementation of A+ for verifiers that use both the qualified E-ID and other verifiable credentials.

Ensuring Trust

The key requirement of a trust infrastructure with the associated ecosystem is to enable verifiability and therefore authenticity of data through human and cryptographic trust. While on a more holistic level, further requirements arise that must be addressed by a governance framework, to ensure this key aspect, some governance and technical measures must be taken within the narrow scope of the discussion paper:

- Every verifier of the ecosystem must be identifiable. Different levels of identification shall be possible, ranging from large commercial participants down to volunteers of hobby associations. Heightened trust levels might require pre-registration or even certification. Different levels of identification will also imply multiple trust registers.
- Proof requests raised against holder wallets shall be logged by the wallet, including requested claims. Proof requests shall be signed to ensure non-repudiation.
- Based on logged proof requests, the holder shall be able to report over-identification attempts (and other patterns or bad practices) of verifiers to an official agency

(anonymously verified or in his name) with minimal effort (by clicking «report» or similar).

Conclusion «Opportunity Switzerland»

Swiss citizens generally trust their federal government and its practices, a level of trust that may not be present in other countries. Therefore, it is important that we establish a **balanced foundation that yields swift results AND aligns closely with our core values**. The infrastructure shall be designed to utilize the most powerful methods and mechanisms available at any given time, that protect privacy, prevent correlation and linkability, while also being sustainably operable and adaptable by the public and private sectors and civil society.

Digital Identity and trust infrastructure capabilities are **key enablers of the Swiss digital economy**, so it must be recognized that their **adoption within businesses requires special emphasis and systematic support.** A trustworthy and diverse set of services inside the wallet app(s) is vitally important for the adoption by society and the creation of socio-economic value. A systematic approach to these aspects of adoption support must be planned for.

One of Switzerland's superpowers, is its **national ability to contribute to develop, evaluate and adopt new cryptographic primitives through its excellent research facilities**. The approach presents an opportunity for Switzerland to take a leading role in this field, to actively contribute to the decision making of standardization bodies and hardware manufacturers and, potentially, fellow European governments. Independent research helps to level the playing field and reduce dependencies on large technology corporations and foreign research institutions like NIST.

Not being an EU member, Switzerland has less dependencies on other stakeholders and has hence the flexibility to **leap ahead and gather practical experiences** with the emerging trust technologies, from which all stakeholders will benefit in the long run.

Appendix

Official response submitted by DIDAS.

DIDAS Responses to Consultation Questions

Which scenario would you prefer?

Scenario A

For what reason do you prefer that scenario?

Clarifications

Scenario A **must** implement mandatory extensions to mitigate known shortcomings (hereinafter referred to as A+):

- Issuing credentials in separate variants:
  - Qualified – mainly for official purposes, stricter, i.e. with identification process, strong cryptographic holder binding in hardware, etc.
  - Substantial – mainly for commercial purposes, less strict owner binding, more convenient.
- Addressing unlinkability by using ephemeral credentials (i.e. dynamically generated credentials, in this context with no or restricted reuse).
- Architecture must be multi stack capable to facilitate evolution (scenario B, mDL and other options).
- Financial coverage must be ensured for **all** mandatory extensions.

Reasons

- Pragmatic
- Proven technologies
- Large communities
- Lower complexity and project risk
- Doable until 2026
- Achieves important privacy and security requirements if amended in listed areas (i.e. ephemeral credentials, privacy preserving revocation, etc.).
- EU compatible
- Mandatory extensions to avoid potential criticisms in the political process.

Do both scenarios fulfil your expectations?

No

What major risks do you foresee?

Clarifications expectations

- Both scenarios have weaknesses
- A+ is the approach which minimizes weaknesses and complexity and therefore keeps the implementation risk of the project manageable.

Risks

- Additional complexity of A+
  - Parallel credential issuing
  - Higher UX complexity due to credential variants – must be hidden from users
  - Ephemeral credentials
- Financing does not cover mandatory extensions of A+ scenario.
- Other options (e.g. scenario B, others) will either be never realized or only with a significant, undesirable delay.

Which «red lines» should not be crossed? Where is no compromise conceivable for you?

- Gaps in privacy preservation for qualified credentials.
- Not providing a qualified level (in what form soever), as this would prevent achieving the political goals for the national E-ID.
- Not providing substantial level, because this would negatively impact adoption by the private sector.
- Inflexible technical specifications and technical infrastructure which prevents evolution as the field progresses.
- Weaking SSI principles which could prevent an ecosystem of credential issuers and verifiers (ambition Level 3).

Additional remarks

Using qualified and substantial in parallel must be complemented with additional measures:

- A mechanism to ensure that only authorized verifiers are allowed to request qualified credentials, e.g. government bodies, healthcare organizations, financial institutions, etc.
- E-ID must be provided both as qualified and substantial credential. The substantial E-ID shall only contain a subset of claims (e.g. AVS13 not included).

Switzerland shall seize the opportunity to establish focused research and implementations for developing and progressing cryptographic technologies, leading the field and contributing to international decision making.

More in-depth information is provided in our separate statement document.

Official Sender

DIDAS – Digital Identity and Data Sovereignty Association

Campus Zug Rotkreuz
Surstoffi 1
CH-6343 Rotkreuz

Your Email

info@didas.swiss

Von: Ritscher Leonie <leonie.ritscher@economiesuisse.ch>
Gesendet: Freitag, 12. Januar 2024 17:09
An: Rauschenbach Rolf BJ <rolf.rauschenbach@bj.admin.ch>
Betreff: AW: Konsultation "Technologie-Entscheidung für die E-ID" - Verlängerung der Antwortfrist, Übersetzungen des Diskussionspapiers

Sehr geehrter Herr Rauschenbach

economiesuisse unterstützt eine Umsetzung der E-ID auf Basis eines technologieneutralen Rechtsrahmens, wobei in der konkreten Umsetzung die technischen Mittel genutzt werden sollen, welche die Zielsetzung einer stabilen und das Vertrauen stärkenden Infrastruktur verfolgen und damit die erforderliche Datensicherheit bieten.

Nur bei Verwendung einer Technologie, welche von den Nutzern als vertrauenswürdig anerkannt wird, ist davon auszugehen, dass die E-ID akzeptiert und damit auch genutzt wird. Für eine detailliertere Stellungnahme verweisen wir auf die Eingaben unserer Mitglieder und insbesondere digitalswitzerland und Swiss Fintech Innovation.

Bei Fragen sind wir gerne für Sie erreichbar.

Mit besten Grüssen und ein schönes Wochenende

Lukas Federer & Leonie Ritscher

economiesuisse
Hegibachstrasse 47, 8032 Zürich
D: +41 44 421 35 46
M: +41 79 743 90 23
leonie.ritscher@economiesuisse.ch

Discussion Paper: E-ID initial technology decision

We really appreciate the work of the E-ID team and the possibility to give feedback to this discussion paper. This is the right way to implement a trusted solution.

Which scenario would you prefer?

We don't see this decision as a technical one, it is much broader. We need to consider the social acceptance rate, the interoperability, the possible use cases. Under consideration of these aspects, we prefer Scenario A, BUT with the vision to enhance it over time considering the adoption of the E-ID infrastructure.

Scenario B is too early from our perspective. It contains the BBS+ signature scheme which is not approved by any standard institutes like NIST, ISO or BACS.

We propose a roadmap based on Scenario A to fulfill the ambitious start of the E-ID in 2026. The migration plan for technological weaknesses is part of the roadmap and is necessary for the adoption of the E-ID Infrastructure.

To start, we propose Scenario A, with an additional data protection policy backed by e.g. Federal Data Protection and Information Commissioner (FDPIC). The policy should ensure that verifier, do not track the status list activities (could detect a revocation of a verified credential) and if violated the verifier would be fined. This is needed step to avoid data privacy issues. In the picture below, we visualized the introduction of the policies.

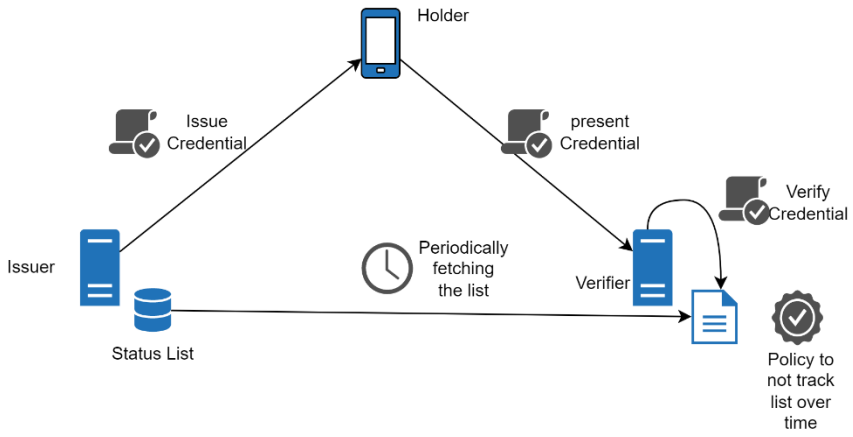

Figure 1: Visualization of the policy to ensure privacy with status list for revocation.

In the beginning, we expect the adoption on ambition levels 1 and 2, which means applying these policies wouldn't be a problem. An audition instance is needed for ambition level 3. In parallel, the standardization for BBS+ or other signature scheme candidates are ongoing to enhance the technological

backed privacy of the SSI concept. In 2028, we assume the technology will have evolved and additional standards and revocation scheme could be experimented with to ensure the privacy by design of the SSI concept. In 2030, we think that a zero-knowledge proof signature scheme will exist and be mature enough to be part of the infrastructure. With EU compatibility in mind, we see the use of SD-JWT, especially for high Level of Assurance (LoA) VCs as mandatory, while Json-LD could be used for other credentials. On the long term, a more privacy preserving revocation method should be adopted to eliminate the current technological weakness of credential revocation tracking. In Figure 2, we visualize a possible journey.

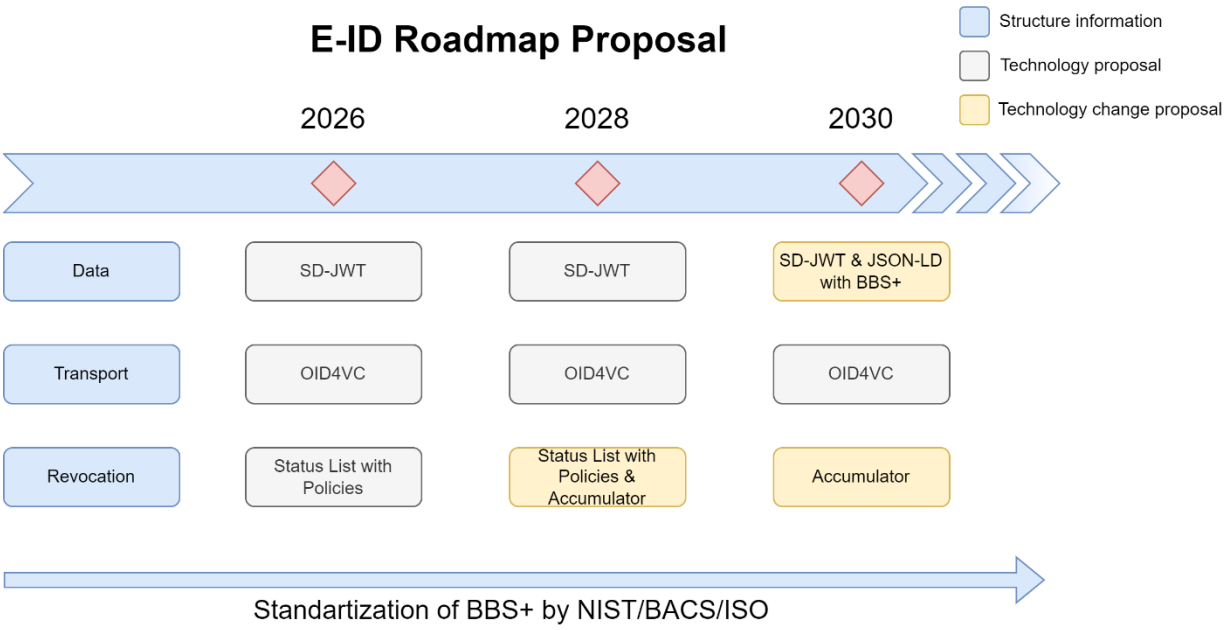

Figure 2: Visualization of the E-ID technology adoption.

The migration to new verifiable credential data structure and revocation method is necessary and we assume the migration will be based on step-by-step reissuance of the credentials. This means, the credentials of the first wave, need to have a shorter expiration (two-three years), to be able to modify the E-ID Stack without too much legacy to maintain.

Further changes regarding transport protocol, credential data structure, which are not considered yet should be applied based on standardization and security level.

For what reason do you prefer that scenario?

We prefer Scenario A, as it start with simple solution that can be migrated afterward. The concept itself is based SSI which gives it the potential to be private by design. It currently has some privacy issues which can be solved with utilization policies and later enforced by technology.

It is also motivated by the short implementation phase for the E-ID. It would support the high LoA of the E-ID with hardware based key material and is compatible with the EU choosen architecture. The privacy issues can be targeted via policies by law enforcement and later with technology. The migration will require re-issuance of credentials, but with minimal interaction from the Swiss population.

Do both scenarios fulfil your expectations? YES or NO

Our expectations are to get an interoperable SSI ecosystem which technically enforced privacy.
From our perspective, both scenarios do currently not fulfil our expectations., but we need to start and show the way on how to adopt SSI in the future.

Those scenarios are not final, and we suggest building on a common base and do focus on the future journey of the E-ID and the SSI ecosystem.

Finally as side note, there are some special cases like the driver license. In the USA there is strong movement to adopt the ISO standard mDL to ensure worldwide interoperability. But to be able to adopt mDL on iPhone and be compatible with the Hardware already introduced by TSA, it is necessary for Apple to open the now restricted APIs to their NFCs chips to make it feasible on a technical level. Otherwise, we would be forced to use the Apple Wallet for driver licenses.

What major risks do you foresee?

Major risks are:

- EU giving up / no budget left, which is possible, as Germany lost a lot of budgets.
- Not finished in time, so all the communication to prepare the citizens would just lower trust of people.
- International incompatibility, people are travelling a lot, and Switzerland is a country with a lot of frontier workers. An interoperability with EU is mandatory and need to be implemented, regardless of chosen scenario.
- No usage of the ecosystem, Only E-ID in the wallet, without any need, will not adopt to it. An adoption plan of digital transformation is necessary.
- Apple does not open the restricted APIs of their NFC chips on their iPhones (UX risk and important for the driver license)
- Law is not accepted.

Which “red lines” should not be crossed? Where is no compromise conceivable for you?

The government needs to be at the root of the SSI ecosystem. It enables the first trust registries and provides the first issuer solution to provide and use an E-ID. It is inconceivable that anyone other than the government can manage the infrastructure base.

Additional remarks

Scenario B is not wrong but there are too many uncertainties. With a short and finite deadline, it is important to unify resources with the community and build on top of a first base and improve it over the time to use its opportunities and increase the privacy and usefulness with time while starting with

adoption. As an adoption example, Twint started small and was mostly used by students at the start and slowly grew as one of the top payment methods between people in Switzerland.

The adoption will start slowly and will only increase with increasing trust in the solution and use case to use it.

Should the government build on top of BBS+ which is not standardized yet? How do we manage Backups (only backup low LoA VCs and get access to them with high LoA VC)?

Happy to discuss it further.

Official Sender

Roman Zoun, Michel Sahli, Leo Huber, Simon Dummermuth, Thomas Zangerl

roman.zoun@adnovum.ch, michel.sahli@adnovum.ch, leo.huber@adnovum.ch, simon.dummermuth@adnovum.ch, Thomas.zangerl@adnovum.ch

https://findmind.ch/c/XFvu-a7c6

SWISS E-ID - DISCUSSION PAPER RESPONSE

Prilly , 15th of January 2024

This document is the detailed SICPA response addressing multiple technical sections of the discussion paper published by the e-ID team on November 22, 2023.

The initial discussion paper invites input on two potential scenarios for the technical foundation of the national trust infrastructure, emphasizing aspects like privacy, interoperability, and system maturity. Its purpose is to encourage public discussion and inform decision-making for the e-ID project. Also, it invites the public to give other comments on points which are regarded important; SICPA takes the opportunity to do so. https://github.com/e-id-admin/open-source-community/blob/main/discussion-paper-tech-proposal/discussion-paper-tech-proposal.md

INTRODUCTION

SICPA, as a Swiss technological provider of decentralized identity technology, has been a pioneer in contributing to the self-sovereign identity (SSI) space for more than 5 years. In that regard, SICPA believes that SSI principles bring key benefits when implementing an e-ID system at the national level to citizens providing full ownership and control over their personal data without relying on a third party and enhancing privacy among others.

SSI principles are well aligned with the vision of a Swiss e-ID to have a State issued and operate e-ID that follow the principles of privacy by design, data minimization and decentralized data storage but highly likely is the best approach to implement an e-ID system at national scale in Switzerland.

To reach Ambition Level 3 and foster a truly Swiss ecosystem of attribute-based digital attestations, it's essential to start with foundational credentials such as the Swiss e-ID, coupled with a trusted infrastructure managed and operated by the government. This initial issuance and adoption of the Swiss e-ID is vital to effectively bootstrap a Swiss ecosystem of attribute-based digital attestations that can be extended to multiple verticals with the collaboration between the public and private sectors.

Finally, SICPA welcomes the high-quality e-ID law draft proposed, as it constitutes a robust basis and establishes the principles for a promising Swiss state-issued e-ID and Swiss-operated trust infrastructure as a foundational cornerstone to bootstrap a Swiss ecosystem of attribute-based digital attestations reaching Ambition Level 3. SICPA also appreciates the open, iterative, inclusive, and collaborative approach that the federal government is taking to consult and involve the different sectors of Swiss society to gather feedback on legislative, societal, and technological aspects of the Swiss e-ID initiative.

SICPA'S RESPONSES TO THE SWISS E-ID QUESTIONNAIRE

First, SICPA is pleased to directly address the questions posed by the Swiss e-ID team. It's important to note that, in addition to responding to these questions, this document also offers additional feedback on various aspects related to the positioning paper.

1 - Which scenario do you prefer?

SICPA prefers scenario A.

2 - For what reason do you prefer that scenario?

As a disclaimer, SICPA advocates for a system that supports multi-protocol, multi-format, and multi-signature capabilities, recognizing its flexibility to accommodate a wide range of use cases. Furthermore, SICPA endorses an iterative approach, initially focusing on a limited set of specifications (Scenario A) to address basic use cases with moderate interoperability, and progressively refining these specifications as they evolve.

Answering the question, SICPA thinks that scenario A is the good starting point due to several reasons.

- **Maturity**: When considering credential exchange protocols and formats for both scenarios, implementations and standards are not yet mature enough (Please see maturity section below for a more detail explanation). However, RSA and ECDSA signature schemes, having been widely used and thoroughly tested in various cryptographic applications over many years, can be considered mature. In contrast, for Scenario B, SICPA thinks that an approach based on JSON-LD verifiable credentials using zero-knowledge proofs is still not mature.
- **Simplicity**: SD-JWT is type of verifiable credentials built upon established web primitives. RSA and ECDSA are well-established and widely implemented across cryptographic libraries and systems. Therefore, regarding implementation and integration into existing systems, Scenario A is likely simpler due to its maturity and widespread use of the underlying technical building blocks.
- **Interoperability**: One of the key objectives of the Swiss e-ID eco-system is to be as much as possible compatible with the European Digital ID framework (according to ARF specifications). This will allow the citizens, governments and the industry to exchange personal data seamlessly across the continent (e.g. travels, etc…). This will obviously allow adoption and scalability from the beginning and ensure efficiency gains for all stakeholders from the very beginning.
- **Support for hardware-backed keys**: Support for hardware-backed keys is necessary to protect against certain attack vectors such as verifiable credential duplication, which is essential for achieving a Level of Assurance High.

3 - Do both scenarios fulfil your expectations?

Yes, SICPA is open to both scenarios as the choice of protocol, credential format, or signature scheme will largely depend on specific use cases or requirements. Hence, a system allowing multi-protocol, multi-format, and multi-signature capabilities is desirable for its flexibility to accommodate a wider range of use cases.

SICPA, as a SSI technology supplier, advocates for a 'multi' broad approach in a domain still emerging in standards and implementations. This flexibility allows bridges between different emerging standards, could greatly benefit establishing a Swiss e-ID ecosystem based on SSI principles. SICPA's experience in building solutions that focus on the discoverability of capabilities in a multi-technology environment confirms the technical feasibility of this approach.

However, it's acknowledged that this approach may introduce certain complexity at the cost of flexibility. Also already mentioned SICPA believes that Swiss e-ID system should be inherently privacy-preserving by design.

4 - What major risks do you foresee?

To effectively manage risks in the future Swiss e-ID ecosystem, tailored approaches are essential. The provided risk / approach table outlines several potential risks and corresponding strategies to address them:

Risk	Approach
Complex and variable technology with Uneven Maturity: The SSI field is marked by complex, evolving technologies of varying maturity levels.	Simplify carefully: The approach is to simplify the technical stack without losing the essence: It involves initially selecting a subset of building blocks that, with 20% of the effort, can achieve 80% of the desired results.
Evolving SSI specifications: As SSI standards are still in development.	Freeze, Deliver, Repeat: This approach involves establishing temporary standards, implementing solutions based on these standards, and iteratively refining them as specifications evolve. Initially, the focus is on a subset of specifications to address basic use cases with moderate interoperability and adoption. Subsequently, the rollout of next-generation specifications is undertaken, aiming for wider adoption. The final stage progresses further, targeting complex use cases and achieving strong interoperability with technical tweaks. Successful evolution of the intermediate solution will be dependent on the existence of sufficient incentive for the actors who have to pay the cost of change.
Practical vs. theoretical Interoperability: There's a gap between theoretical interoperability and practical, useful interoperability.	Interop Profiles: Developing interoperability profiles ensures that different systems can work together effectively in real-world applications. Additionally, the necessity of formal testing and a defined target with multi-vendor commitment is important, in contrast to plugfests which can be artificial and ephemeral. It must be noted that the proposed set of specifications for OpenId4VC are very broad in scope, more details in the technical section.
Unique cybersecurity challenges in SSI: The cybersecurity needs in SSI are distinct and critical.	Security Roadmap: Creating a detailed and robust security plan tailored to the unique challenges of SSI systems.
Long-term sustainability needs attention: The need for a long-term perspective in the development of SSI solutions.	Permanence Plan: Establishing strategies for the long-term viability and sustainability of Swiss trust infrastructure and standards.

Risk	Approach
Lack of concrete and enforceable governance to counter over-identification	Governance framework: define what constitues a legitimate scenario for identification, what kind of information these scenarios call for and who is entitled to ask for verification in these instances. The enforceability is critical to remove the burden of deciding what calls for legitimate identification from the end-user

5 - Which "red line" should not be crossed?

SICPA believes that the Swiss e-ID system should inherently preserve privacy by design, prioritizing unlinkability and data minimization. Achieving this goal might not be feasible initially due to short timelines and the lack of maturity in certain standards, but it should be established as a long-term goal. This principle should serve as a guiding standard for the evolving Swiss e-ID system. If technical limitations prevent us from initially meeting our goals, we should clearly communicate these limitations to citizens and industry.

This transparency will inform all stakeholders about the risks associated with using the early version of the Swiss e-ID, allowing them to make informed decisions about its application, especially in cases where data privacy is critical, such as health-related scenarios. They may also choose to wait for future releases with enhanced data protection.

OTHER SICPA'S CONSIDERATIONS

Maturity

When it comes to credential exchange protocols and credential formats, we could generally say that the maturity of standards and their implementation in both scenarios is still not mature, with the exception of W3C VCDM 1.1 and JSON-LD 1.1 standards, that are W3C recommendations.

Regarding signature schemes in both scenarios, there is a key differentiator. On one hand, RSA and ECDSA are widely used and thoroughly tested in various cryptographic applications over many years, providing a strong track record of reliability and security, assuming proper implementation and key management practices. On the other hand, BBS+, while showing promise and significant potential in privacy-preserving use-cases, does not yet have the extensive track record of RSA and ECDSA.

Privacy

SICPA believes that e-ID systems following SSI principles should be inherently privacy-preserving by design, prioritizing unlinkability (increased cost of correlation) and data minimization.

Advanced cryptographic techniques like zero-knowledge proofs are worth the evaluation, including BBS+ in scenario B, which offer promising privacy-enhancing traits like selective disclosure, unlinkability of VC signatures and credential holders, and proof of possession. Furthermore, two vital privacy-preserving features not considered in scenario B are predicate/range proofs and privacy-preserving revocation.

Privacy should be a priority; however, SICPA is not exclusively advocating for Zero-Knowledge Proofs as the only approach to enhancing privacy. A more detailed and nuanced analysis is necessary. We hold that the selection of privacy-enhancing technologies must be informed by specific use-cases and requirements. This includes carefully assessing the balance between the cost correlation and other elements such as security, compliance, standardization, among others. Consequently, we believe multiple credential types, such as SD-JWT, could co-exist for different use-cases, in line with what is currently proposed by the European ARF framework, which acknowledges and supports multiple types of credentials (Type 1 and Type 2) for a range of needs.

Governance

Digital identity will drastically decrease the cost of identification. It is crucial for a government-level proposition to introduce a strong regulation on what situations legitimately require such a strong identification of individuals. It is undesirable for data authentified by official and governmental organisms to fall under the same, relatively lax, umbrella as "personally identifying data". GDPR and similar regulations are not fit for the level of authenticity digital identity brings.

Interoperability

Ensuring that the Swiss e-ID is functional and widely accepted beyond Switzerland's borders is a crucial aspect. From a technical interoperability perspective, achieving interoperability with the EUDI wallet Architecture Reference Framework (ARF), would be a desirable outcome.

The discussion paper lays out 2 different scenarios, being scenario A aligning with the European Union's technical direction, particularly the Architecture Reference Framework (Type 1).

It's important to note that interoperability is necessary at the edge, or in other words, when a holder generates a proof requested from a relaying party. This implies that within an SSI ecosystem, the issuance of a foundational identity can be specific to the Swiss e-ID's chosen technical standards, without interoperability concerns.

For use-cases requiring from the holder to provide a proof to a non-Swiss verifier, different technical approaches can be utilized. One approach is issuing multiple copies of the same credential in different formats. This "Multi-VC" type approach could issue dual credentials, one interoperable with Swiss e-ID technical specifications and another with EUDI wallet technical specifications. This approach is technically feasible with issuance protocols such as OpenID4VCI or DIDCOMM.

Another interoperability approach involves mapping between different credential formats, enabling conversion from one to another and facilitating compatibility across ecosystems. This method essentially acts as a translator, ensuring credentials remain usable and recognized in varied technical environments. However, a limitation is the impracticality of direct conversion due to the diverse underlying signature schemes in various ecosystems.

Decentralized Identifiers (DIDs)

Decentralized Identifiers (DIDs) are a new type of globally unique digital identifier that enables self-sovereign identity through decentralization, resolvability, persistence, and cryptographic verifiability.

DIDs bring an added layer of abstraction, flexibility and autonomy to this concept. Unlike traditional identifiers that remain tightly anchored to a specific system or central authority, DIDs can be rooted across a broad spectrum of platforms, from blockchains to traditional web infrastructures, or even locally on devices.

SICPA views DIDs as a fundamental pillar in enabling self-sovereign identity principles, serving as a versatile and innovative tool in digital identity to establish secure, authenticated, and user-controlled digital interactions.

Decentralization and self-sovereignty are key aspects that enable DIDs. In this context, the Swiss base-registry, functioning as a Verifiable Data Registry (VDR), will play a crucial role, particularly in anchoring, storing and resolving future new Swiss-based DID methods. VDR approach to decentralization, governance, and transparency, along with other factors, will be key when potentially designing did methods based on the Swiss base-registry.

Overall, although not included in the different scenarios, SICPA is very enthusiastic and encourages the adoption of DIDs as an integral pillar of the Swiss E-ID. This adoption aims to enable trusted digital interactions anchored in the Swiss trust infrastructure.

Technical Expertise and SICPA learnings

SICPA has worked and productized multiple technologies and implement standards included in the discussion paper. The following section describes some of our learnings.

DIDComm Messaging

DIDcomm is a framework that enables the creation of secure, private, decentralized protocols on top of DIDs that support any transport mechanism.

DIDComm presents several compelling privacy-preserving advantages over traditional communication methods. These advantages come “out-of-the-box" with DIDComm, which prevents making mistake when implementing them. For example, it offers end-to-end encryption, ensuring that messages can only be read by the intended recipients. This level of security is a significant improvement over many current messaging protocols that may not offer such robust encryption. Additionally, DIDComm facilitates interoperability across different systems and platforms, as it does not enforce the transport medium. This allows using DIDComm on top of different stacks (mobile-to-mobile, Web, etc) simpler, which saves some implementation time.

However, we also experienced some drawbacks when using DIDComm Messaging. A primary concern is its relative lack of maturity and widespread adoption. For instance, the transition to DIDComm version 2 has been slow, which shows hesitance or challenges in adopting the latest standards. Also, the libraries and tools available for DIDComm are still in their early stages. They often lack the robustness and alignment seen in more established technologies, leading to potential integration and compatibility issues.

It's also worth noting that DIDComm introduces new concepts and paradigms that require a learning curve. For example, in scenarios like peer-to-peer exchanges between mobile devices, the setup of mediators or relayers is necessary. This necessitates a deeper understanding of the underlying mechanisms and a change of mindset compared to more traditional designs, which can be a barrier to entry for some users.

Sumarizing, While DIDComm does provide secure communication, its purpose is broader. It enables privacy-respecting, end-to-end encrypted interactions directly between parties, leveraging decentralized identifiers (DIDs). It's not just about securing messages but about enabling a new paradigm of trust and interaction in digital communications.

OpenID for Verifiable Credentials

- While under active development, the OpenId4VC specifications are not mature. They are also catch-all specifications meant to deal with an as large as possible range of scenarios for interactions between edge-holders and centralized issuers/verifiers. This means that a proper interoperability profile should decide the scope of what is being used from the specification carefully.
- Returning to the topic of 'interactions between edge-holders,' it's important to note that the OpenId4VC specifications currently do not target 'cloud interactions' significantly. As of now, these interactions are somewhat of an afterthought in the specifications. This aspect is pertinent in various public use cases, including scenarios involving organizations and company identifications, where cloud interactions are anticipated.
- Because OAuth 2.0 and OpenID are widely adopted building on top of these standards makes sense and provides seemingly easy way to introduce Verifiable Credential concept to existing deployments but at the same time makes it difficult to build new platforms and solutions as the number of related specs can be overwhelming and can lead to insecure implementations.
- Attack surface now includes all specifications that OpenID 4 VC family references.

W3C VCDM and JSON-LD

Verifiable Credentials Data Model (https://www.w3.org/TR/2022/REC-vc-data-model-20220303/ v1.1 W3C Recommendation at the time of writing)

Specification for Verifiable Credentials in JSON or JSON-LD format, with the JSON-LD format enabling the properties offered by the Linked Data(https://www.w3.org/TR/ld-glossary/#linked-data).

This brings the possibility to clearly define terms that are part of a given JSON-LD credential, enabling a context(https://www.w3.org/TR/2022/REC-vc-data-model-20220303/#contexts) for human and machine-readable credential data, promotes interoperability between different data formats and structures, supports language-tagged strings enabling creation of multilingual credentials, easy to understand and use for those familiar with JSON. With JSON-LD being a widely used standard there is a robust ecosystem of software libraries for validation, parsing and processing of JSON-LD Verifiable Credentials. This supports Ambition Level 3 where multiple parties coexist, issue, hold, and verify credentials in an ecosystem and allows for easier bridging of separately evolving ecosystems as well.

Considerations Include: the context being located on infrastructure that is optimized for high availability, since failing to fetch a given context results in an inability to verify credential authenticity (this can be mitigated by caching of the context by system actors). The VCDM v2.0 (W3C Working Draft https://www.w3.org/TR/2024/WD-vc-data-model-2.0-20240110/ at the time of writing) aims to resolve Ecosystem Compatibility (https://www.w3.org/TR/2024/WD-vc-data-model-2.0-20240110/#ecosystem-compatibility), it states that if a Verifiable Credential can be transformed into a "conforming document" they can be considered compatible with the W3C Verifiable Credentials ecosystem.

Note that at the time of this writing VCDM v2.0 is only a Working Draft and will undergo changes before it transitions to a Recommendation. It is worth considering that in the v2.0 the context property is a MUST for all credentials that aim to be conforming and it might be worth future-proofing the context definitions for credentials that are being issued via VCDM v1.1.