Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP
Office fédéral de la justice OFJ

14 juin 2024

Consultation concernant la décision sur la technologie à utiliser pour l'infrastructure de confiance et l'e-ID

Synthèse des résultats

Table des matières

Résumé

Le Conseil fédéral a adopté le message concernant la loi fédérale sur l'identité électronique et d'autres moyens de preuves électroniques (LeID) lors de sa séance du 22 novembre 2023. Cette loi confie à la Confédération la responsabilité de l'émission de l'e-ID (moyen électronique d'identification des personnes) et l'exploitation d'une infrastructure de confiance à cet effet. Il est prévu que les premières e-ID soient délivrées dès l'entrée en vigueur de la loi, début 2026. Il est crucial, pour pouvoir respecter ce délai, de prendre aussi vite que possible une décision sur la technologie à utiliser.

Afin de fournir une assise à cette décision, l'administration a mené une consultation publique sur un document de travail qui présentait et analysait deux scénarios pratiques. Chacune de ces solutions a des avantages et des inconvénients. Dans le premier scénario, la Suisse suivrait en grande partie l'orientation technique de l'Union européenne (UE). Dans le deuxième scénario, elle utiliserait une technologie qui offrirait aux utilisateurs une protection encore plus grande de leur sphère privée.

Suite à la consultation, 97 avis ont été rendus par les autorités, les partis politiques, les organisations et les particuliers. Les préférences sont à peu près équilibrées entre les deux scénarios. La décision exige une complexe mise en balance de différents facteurs, parmi lesquels la protection des données, la sécurité, l'interopérabilité et la faisabilité technique.

1 De quoi s'agit-il ?

Après le rejet de la loi fédérale sur les services d'identification électronique lors de la votation populaire du 7 mars 2021, le Conseil fédéral a chargé le Département fédéral de justice et police de poser les bases d'un moyen d'identification électronique sûr émis par l'État, en collaboration avec la Chancellerie fédérale et le Département fédéral des finances. En outre, le Conseil national et le Conseil des États ont déposé six motions de même teneur, émanant de tous les groupes parlementaires, pour demander la création d'un système géré par l'État qui permette de prouver son identité en ligne.

L'Office fédéral de la justice (OFJ), soucieux d'associer dès le début les milieux intéressés à l'élaboration de la nouvelle loi, a mené à l'automne 2021 une consultation publique informelle. Se fondant sur les résultats de cette consultation, le Conseil fédéral a défini les principes de la nouvelle e-ID étatique, le 17 décembre 2021. Il a mené une procédure de consultation du 29 juin au 20 octobre 2022 sur un avant-projet. Le projet de loi et le message ont été adoptés le 22 novembre 2023. Le Conseil national a approuvé la loi sur l'e-ID le 14 mars 2024 par 175 voix contre 12 et 2 abstentions.

Il est prévu que les premières e-ID puissent être délivrées dès l'entrée en vigueur de la loi, début 2026. Il est crucial, pour pouvoir respecter ce délai, de prendre aussi vite que possible une décision sur la technologie à utiliser.

Afin de bénéficier davantage des vastes connaissances et du réseau de la communauté suisse de l'e-ID, l'équipe de projet e-ID a créé un cercle consultatif technique (Technical Advisory Circle, TAC), qui a conseillé l'OFJ dans l'élaboration du document de travail. Ce document porte sur les éléments suivants :

- un aperçu du cadre : vision de l'OFJ et rappel du contexte européen ;
- les principes ayant présidé à la conception de l'e-ID et de l'infrastructure de confiance selon le projet de loi ;
- les critères de décision ;
- deux scénarios possibles : suivre l'orientation technique de l'UE / renforcer davantage la protection de la sphère privée.

Le document de travail a été publié sur GitHub le 1er décembre 2023 dans sa version anglaise originale ; les traductions allemande et française ont suivi. L'invitation à participer à la consultation a été envoyée le même jour, via la newsletter e-ID et par courriel. Les questions posées étaient les suivantes :

- Quel scénario préférerez-vous ? Et pour quelle raison ?
- Les deux scénarios répondent-ils à vos attentes ?
- Quels risques majeurs prévoyez-vous ?
- Quelles sont les « lignes rouges » à ne pas franchir ?

Il était possible de répondre à ces questions sur un formulaire Web, auquel on pouvait ajouter des commentaires et compléments. La présente synthèse tient compte de toutes les 97 réponses reçues jusqu'au 22 janvier 2024.

2 Résultats

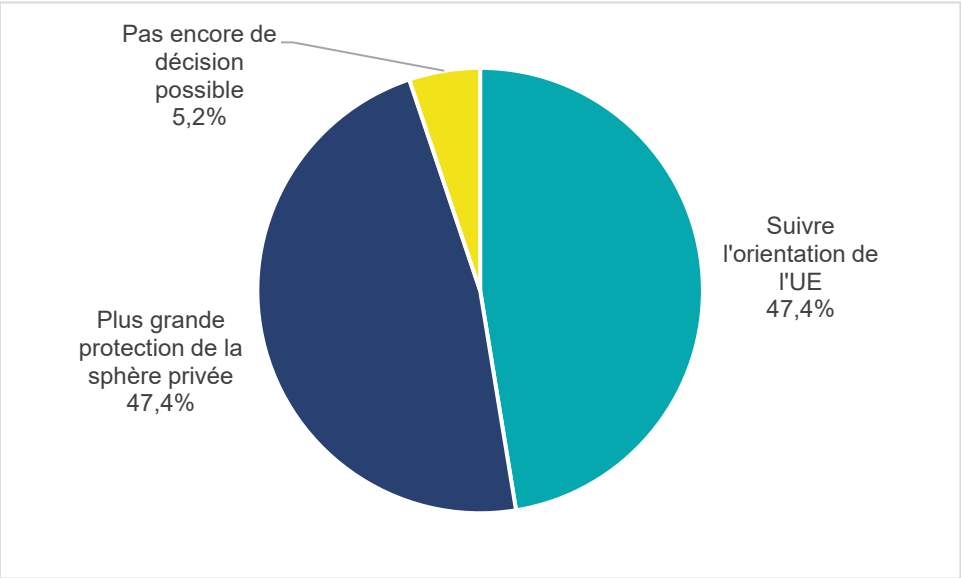
97 organisations ou personnes ont pris part à la consultation. Parmi elles, 85 ont simplement rempli le formulaire Web, 6 l'ont complété par un avis séparé et 6 autres ont pris position sur papier libre.

Les résultats de la consultation ont été publiés sur GitHub le 7 mars 2024, sous forme d'un tableau Excel (réponses sur formulaire Web) et d'un PDF (avis sur papier libre).

La liste des participants à la consultation se trouve en annexe.

2.1 Quel scénario préférerez-vous ? Et pour quelle raison ?

L'exploitation numérique des préférences exprimées montre que 46 participants (47,4 %) souhaitent suivre l'orientation de l'UE tandis que 46 (47,4 %) privilégient une plus grande protection de la sphère privée. Il ressort des 5 autres réponses (5,2 %) qu'il n'est pas encore possible de prendre une décision sur la base des informations disponibles (voir graphique 1).



Graphique 1 : Préférences brutes

Parmi les tenants d'une orientation vers l'UE, on trouve en particulier les participants suivants : cantons d'Appenzell Rhodes-Intérieures, Bâle-Campagne, Bâle-Ville, Obwald, St-Gall, Thurgovie (Migrationsamt), Valais, Vaud, Zoug, DIDAS, SICPA SA, Switch, Procivis AG, Union des villes suisses, Swisscom SA, Ergon Informatik AG, Adnovum AG, Educa, Chemins de fer fédéraux, Association suisse des officiers de l'état civil, Office fédéral de la santé publique. Leurs motifs sont notamment les suivants :

- l'interopérabilité avec l'UE ;
- le recours à une technologie et une cryptographie éprouvées, la résilience post-quantique ;
- la simplicité, le moindre coût et la rapidité de la mise en œuvre ;
- la grande taille de la communauté des développeurs, la rapidité de la mise en place de l'écosystème.

Les tenants d'une plus grande protection de la sphère privée sont notamment les suivants : cantons d'Argovie, Genève, Fribourg, Neuchâtel, Lucerne, St-Gall (Fachstelle für Datenschutz), Soleure, Schwyz, Thurgovie (Departement für Inneres und Volkswirtschaft, Kompetenzzentrum für Digitale Verwaltung), Les Vert.e.s suisses, Parti socialiste suisse, Abraxas Informatik AG, Parti pirate suisse, CH++, Ubique, Swiss FintechInnovations, EPFL, Référendum sur l'e-ID, Société numérique, La Poste Suisse SA & SwissSign SA, digitalswitzerland, IBM Research, Swico, Information Security Society Switzerland, Vereign AG, Swiss Data Alliance,

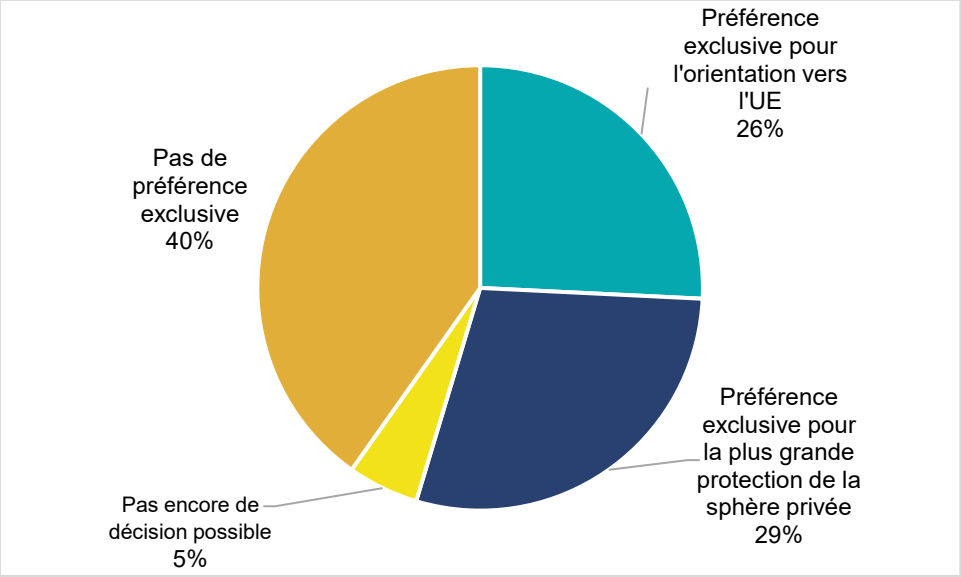
Union suisse des arts et métiers, Health Info Net AG, syndicom, Organisation des Suisses de l'étranger, economiesuisse. Leurs arguments sont les suivants :

- Une plus grande protection de la sphère privée, en particulier la dissociabilité (*unlinkability, traceability, non-correlation*). Pour illustrer la dissociabilité : une personne prouve, lors d'une première transaction, qu'elle est majeure, sans dévoiler d'autres attributs tels que son nom ou sa date de naissance exacte. Le vérificateur reçoit non seulement l'information « personne majeure », mais aussi un élément cryptographique qui rend cette preuve vérifiable et unique. Si la dissociabilité est assurée, il ne pourra pas, lorsque la même personne présente de nouveau la preuve qu'elle est majeure, savoir que cette deuxième transaction est faite par la même personne. Il est clair que si la dissociabilité n'est pas garantie, c'est-à-dire si les données sont associables, il est facile d'établir le profil d'une personne ;
- L'acceptabilité politique, un moindre risque de référendum ;
- L'autonomie par rapport à l'étranger et notamment à l'UE, dont les plans ne sont pas encore clairs ;
- La possibilité pour la Suisse d'être pionnière au niveau mondial en matière de protection de la sphère privée.

Cinq cantons déclarent ne pas être en mesure de prendre une décision sur la base des informations disponibles : Appenzell Rhodes-Extérieures, Berne, Glaris, les Grisons et Zurich.

2.2 Les deux scénarios répondent-ils à vos attentes ?

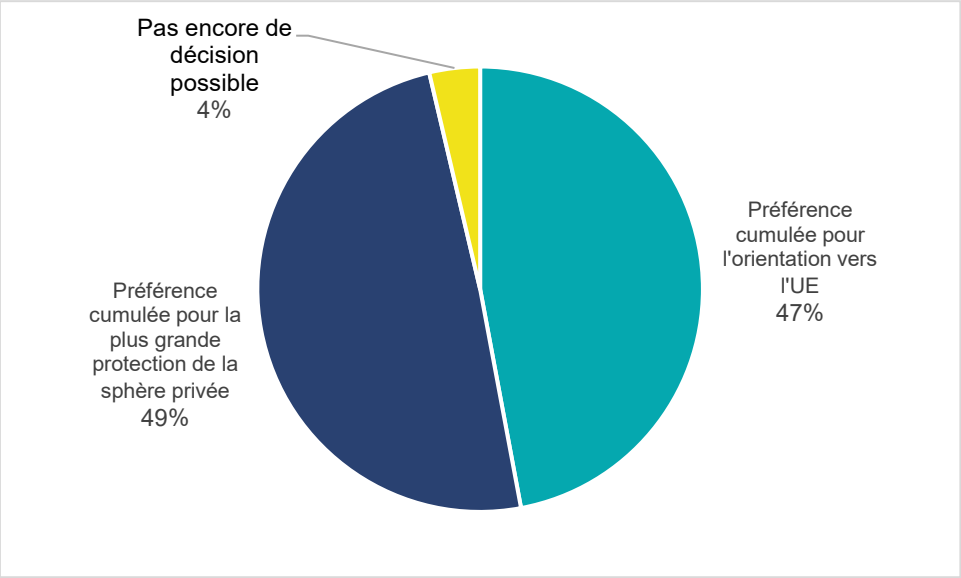
L'analyse des préférences exclusives donne les résultats suivants : 25 participants (26 %) sont exclusivement favorables à l'idée de suivre l'orientation de l'UE tandis que 28 autres (29 %) souhaitent exclusivement une plus grande protection de la sphère privée. Ils sont 5 (5 %) à estimer impossible de prendre une décision sur la base des informations disponibles. 39 (40 %) n'ont pas de préférence exclusive (voir graphique 2).



Graphique 2 : Préférences exclusives

Souhaitent exclusivement suivre l'orientation de l'UE, notamment : canton d'Obwald, Office fédéral de la santé publique, Fédération suisse des avocats, DIDAS, Union des villes suisses, Interpension, Procivis AG, AdNovum AG, Chemins de fer fédéraux.

Souhaitent exclusivement une plus grande protection de la sphère privée, notamment : les cantons d'Argovie, Fribourg, Lucerne, Soleure, St-Gall (Fachstelle für Datenschutz), Thurgovie (Departement für Inneres und Volkswirtschaft), Parti socialiste suisse, Les Vert.e.s suisses, Swiss Fintech Innovations, Référendum sur l'e-ID, IBM Research, Information Security Society, Union suisse des arts et métiers, syndicom, Société numérique, Vereign AG, Health Info Net AG.



Graphique 3 : Préférences cumulées

L'analyse des préférences cumulées fait apparaître que 64 participants (47 %) envisagent de suivre l'orientation de l'UE comme premier ou deuxième choix. Ils sont 67 (49 %) à avoir la plus grande protection de la sphère privée comme premier ou deuxième choix. Les 5 participants qui estiment impossible de prendre une décision sur la base des informations disponibles ont dans cette analyse un poids de 4 % (voir graphique 3).

2.3 Quels risques majeurs prévoyez-vous ?

Les risques mentionnés dans les avis reçus peuvent être regroupés dans les catégories suivantes :

- Rapidité de décision : certains jugent prématuré de décider de la technologie à employer et craignent qu'une décision trop précoce n'aboutisse à une impasse. D'autres, à l'inverse, estiment qu'une décision trop tardive menace l'e-ID même. Pour eux, l'essentiel est de pouvoir émettre les e-ID aussi rapidement que possible, des ajustements postérieurs étant de toute manière inévitables. Des craintes ont également été exprimées quant aux retards que pourrait prendre le projet si l'on suivait l'orientation de l'UE, au cas où celle-ci ne progresserait pas à l'allure prévue.
- Risques techniques : ils sont plusieurs à avancer que les technologies proposées ne sont pas encore mûres, qu'il manque de normes techniques, que le problème lié aux processeurs quantiques n'est pas résolu, que le projet est trop complexe et qu'il faut donc s'attendre dans le meilleur des cas à une explosion des coûts et à des dépassements de délai. Un problème lié à ceux-ci est la petite taille des communautés qui veulent développer ces technologies. Une autre remarque a été faite concernant les risques techniques : on peut partir du principe que l'on restera dépendant du chemin choisi. Le document de travail évoque la possibilité d'emprunter parallèlement plusieurs voies technologiques (*multistack* ou empilements multiples). Il serait cependant difficile, voire

impossible, si l'on choisit de suivre l'orientation de l'UE, de développer davantage, à un moment ultérieur, la protection de la sphère privée.

- Risques liés au matériel : vu notamment la solution prévue pour la conservation de l'e-ID – les smartphones des détenteurs –, plusieurs ont souligné le danger qu'il y a à dépendre de matériels et logiciels propriétaires, en partie peu transparents. De plus, tous les types de signatures souhaitables ne sont pas forcément pris en charge par les cryptoprocesseurs incorporés dans les smartphones.
- Échec politique : étant donné l'échec de la première loi sur l'e-ID, beaucoup craignent un nouvel échec dans les urnes et préfèrent de ce fait le scénario d'une plus grande protection de la sphère privée. D'autres estiment au contraire que les solutions rattachées à cette variante n'ont au mieux qu'une valeur académique et présentent le risque que l'on poursuive une chimère.
- Isolement de la Suisse : quelques-uns pensent que le choix du scénario avec plus grande protection de la sphère privée séduit ceux qui sont par principe critiques envers les solutions de l'UE et préfèrent que la Suisse fasse cavalier seul.
- Autres risques : les avis reçus évoquent notamment les autres risques suivants : demandes d'identification excessives, risques de fuite de données, manque de convivialité, manque de possibilités d'utilisation.

2.4 Quelles sont les « lignes rouges » à ne pas franchir ?

Les réponses à cette question reflètent les résultats de l'analyse des préférences exclusives. On a vu au ch. 2.2 que 26 % des réponses étaient favorables exclusivement à une solution orientée vers l'UE, et 29 % à une solution protégeant davantage la sphère privée, tandis que 40 % n'expriment pas de préférence exclusive ; 5 % des participants trouvent prématurée une décision.

Logiquement, se détourner de l'UE est qualifié de ligne rouge par quelques participants. De nombreux avis citent comme lignes rouges les compromis en matière de protection des données et de sécurité. À ce sujet, beaucoup évoquent la dissociabilité des preuves, en cas de présentation d'une même preuve à plusieurs reprises.

Dans l'ensemble, on constate toutefois que de nombreux participants se réfèrent à leurs considérations relatives aux risques (voir ch. 2.3) plutôt que de parler de lignes rouges strictes. Ils formulent plutôt des recommandations telles que :

- communiquer de manière transparente les éventuelles concessions – quelles qu'elles soient – et les motiver ;
- donner si possible la préférence aux solutions qui peuvent être adaptées le plus facilement possible aux évolutions futures ;
- toujours garder à l'esprit ce qui est politiquement réalisable ;
- privilégier le scénario qui favorisera le mieux l'adoption de l'e-ID par le secteur privé.

2.5 Autres remarques

En conclusion du formulaire de consultation, les participants étaient invités à faire part de leurs autres remarques dans un champ libre de texte. Les thèmes abordés dans les ch. 2.3 et 2.4 sont fréquemment apparus parmi ces remarques. Les considérations suivantes méritent également d'être relevées :

- L'e-ID devrait pouvoir être émise comme preuve qualifiée et comme preuve substantielle, éventuellement avec des attributs différents.

- Une connexion étroite avec la signature électronique qualifiée, ou du moins un accès fortement simplifié à cette signature, est nécessaire.
- S'il est sans conteste d'une grande importance que l'e-ID soit associée à son titulaire – association de l'utilisateur, de l'appareil, du portefeuille numérique et de la preuve –, cela ne doit pas amener à ce qu'elle soit associée aux firmes informatiques.
- Le développement de l'écosystème – avec de nombreux émetteurs et vérificateurs – a une grande importance ; la Confédération doit prendre ses responsabilités à cet égard.
- La position déjà prépondérante de la recherche cryptographique en Suisse doit être encore accrue en raison de son importance croissante.
- Plusieurs participants offrent leur soutien ou leur coopération dans le développement de l'infrastructure de confiance.

3 Remarques finales

La consultation montre que les préférences entre les deux scénarios proposés sont équilibrées. La décision exige une complexe mise en balance de différents facteurs, parmi lesquels la protection des données, la sécurité, l'interopérabilité et la faisabilité technique.

Les réponses ont également fait apparaître l'excellente compréhension du sujet par les participants. C'est un facteur non négligeable dans la perspective des débats publics à venir concernant l'e-ID et l'infrastructure de confiance et du développement de l'écosystème de preuves numériques.

4 Annexe

4.1 Participants au Technical Advisory Circle

Le Technical Advisory Circle a siégé trois fois en ligne. Les procès-verbaux des rencontres sont publiés sur GitHub :

- 21 septembre 2023 (https://github.com/e-id-admin/general/blob/main/meetings/20230921_TAC_Meetingminutes.pdf).
- 16 octobre 2023 (https://github.com/e-id-admin/general/blob/main/meetings/20231016_TAC_Meetingminutes.pdf)
- 9 novembre 2023 (https://github.com/e-id-admin/general/blob/main/meetings/20231109_TAC_Meetingminutes.pdf)

4.2 Liste des participants à la consultation

Cantons

- Canton d'Argovie
- Canton d'Appenzell Rhodes-Extérieures
- Canton d'Appenzell Rhodes-Intérieures
- Canton de Bâle-Campagne
- Canton de Bâle-Ville
- Canton de Berne
- Canton de Fribourg
- Canton de Genève
- Canton de Glaris
- Canton des Grisons
- Canton de Lucerne
- Canton de Neuchâtel
- Canton d'Obwald
- Canton de Schwyz
- Canton de Soleure
- Canton de St-Gall
- Canton de St-Gall, Fachstelle für Datenschutz
- Canton de Thurgovie, Departement für Inneres und Volkswirtschaft
- Canton de Thurgovie, Kompetenzzentrum Digitale Verwaltung
- Canton de Thurgovie, Migrationsamt
- Canton de Vaud
- Canton du Valais
- Canton de Zoug
- Canton de Zurich

Autorités

- Office fédéral de la santé publique, Division Transformation numérique
- Office fédéral de la santé publique, Section Santé numérique

Partis politiques

- Les Vert.e.s suisses
- Parti pirate suisse
- Parti socialiste suisse

Cercles scientifiques

- Beer, Carolin & Schaller, Patrick & Čapkun, Srdjan (tous EPFZ)
- EPFL
- Fehrensen, Benjamin (BFH)
- HES-SO
- Laube, Annett (BFH)

Autres

- Abraxas Informatik AG, Christian Werder
- Abraxas Informatik AG, Silvano Fari
- Adnovum AG
- Association suisse des officiers de l'état civil
- Organisation des Suisses de l'étranger
- Commission extra-parlementaire Forum PME
- besec.digital AG
- CH++
- DIDAS
- Société numérique
- digitalswitzerland
- economiesuisse
- Educa
- Référendum sur l'e-ID
- Ergon Informatik AG
- FutureITcom GmbH
- gigmade AG
- Health Info Net AG
- Hoewler Consulting
- IBM Research
- Information Security Society Switzerland
- Inova Solutions AG
- Netcetera AG, Veridos AG, Blokverse
- Procivis AG
- Rigiblue
- Samsung Electronics Switzerland GmbH
- Schweidt & Bachmann Schweiz

- Chemins de fer fédéraux CFF
- Fédération suisse des avocats
- Union suisse des arts et métiers
- Union des villes suisses
- SICPA SA
- SORBA EDV AG
- Swico
- Swiss Data Alliance
- Swiss Fintech Innovations
- La Poste Suisse SA & SwissSign SA
- Swisscom SA
- Switch
- syndicom
- Ubique AG
- Vereign AG
- Association eGov-Schweiz
- Association des services de la navigation

Particuliers

- Aeschlimann, Andres
- Anonyme 1
- Anonyme 2
- Anonyme 3
- Anonyme 4
- Anonyme 5
- Blume, Matthias
- Christen, Tobias
- Dunant, Raphaël
- Fiore, Nico
- Furrer, Bruno
- Gfeller, S.
- Grossenbacher, Samuel
- Keil, Hartmut
- Keller, Philippe
- Oeri, Hans-Peter
- Šarinay, Juraj
- Schnyder, Stéphane
- Suvorov, Vasily

4.3 Réponses reçues par formulaire Web

Les réponses reçues par formulaire Web sont publiées sur GitHub sous forme de fichier Excel : https://github.com/e-id-admin/open-source-community/blob/main/discussion-paper-tech-proposal/20240307_discussion_paper_tech_proposal_responses.xlsx

4.4 Avis séparés

Les avis rendus séparément sont publiés sur GitHub sous forme de fichier PDF :
https://github.com/e-id-admin/open-source-community/blob/main/discussion-paper-tech-proposal/20240307_discussion_paper_tech_proposal_additional_statements.pdf