Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP

Office fédéral de justice OFJ
Domaine de direction Services centraux
Unité Informatique juridique

Novembre 2021

Consultation publique sur le document de travail concernant le projet d'identité électronique (e-ID)

Rapport sur les résultats de la consultation publique

Table des matières

Résumé

La consultation publique sur le document de travail concernant le projet d'identité électronique (e-ID) a duré du 2 septembre au 14 octobre 2021. Dans le cadre de la consultation, 60 participants ont déposé une prise de position. Près de la moitié voit la nouvelle tentative d'instaurer l'e-ID comme une chance de faire passer au niveau d'ambition 3 la vision d'une infrastructure numérique de confiance (7 cantons, 2 partis politiques, 14 organisations, 2 hautes écoles et 4 entreprises). L'e-ID n'est, dans un tel écosystème, qu'une preuve numérique parmi d'autres, citées dans les prises de position. L'identité souveraine (self-sovereign identity) a été citée comme technologie sous-jacente privilégiée par une majorité (8 cantons, 2 partis politiques, 11 organisations, 2 hautes écoles et 8 entreprises). Tout en souhaitant une application conviviale et d'une interopérabilité internationale, une majorité soutient le « respect de la vie privée dès la conception » (privacy by design) et la « maîtrise des données par l'utilisateur »; près de la moitié cite explicitement la « minimisation des données ». Les points de vue sur d'autres aspects sont divers et variés surtout en prévision des discussions à venir. De manière générale, les prises de position sont optimistes et se concentrent sur les chances qu'offre la situation actuelle.

1 Généralités

Le 2 septembre 2021, la consultation publique sur le document de travail concernant le projet d'identité électronique (e-ID) a été lancée lors d'une réunion du comité consultatif sous la direction de la conseillère fédérale Karin Keller-Sutter. Elle s'est achevée le 14 octobre 2021 par un débat public sous forme de conférence.

Le présent rapport d'évaluation se base exclusivement sur les prises de position écrites reçues. Étant donné le calendrier et les délais courts pour la déposition des prises de position, seules celles parvenues avant le 4 novembre 2021 à l'Office fédéral de la justice ont été prises en compte.

Les cantons, les partis politiques, les associations faîtières des communes, des villes et des régions de montagne, les associations faîtières de l'économie et les autres milieux intéressés ont été invités à prendre position.

En tout, 16 cantons[1], 4 partis politiques, 21 organisations, 3 hautes écoles et 16 entreprises ont pris position. Le présent rapport se réfère donc à 60 prises de position. Une organisation (l'Union patronale suisse) a explicitement renoncé à prendre position.

Le document de travail concernant le projet d'identité électronique (e-ID), déposé pour consultation publique, fait un état des lieux. Il énumère les exigences politiques (motions), expose les définitions et dimensions possibles pour une future e-ID suisse et les infrastructures nécessaires et explore trois ébauches de solutions techniques.

Afin d'exploiter pleinement les prises de position, trois questions ont été posées:

- Quelles sont les trois principales exigences auxquelles doit satisfaire une e-ID étatique comme moyen d'identification numérique?
- Quels sont les principaux domaines d'utilisation de l'e-ID?
- Quels sont les avantages d'une infrastructure nationale permettant à l'État et aux particuliers de prouver et de contrôler électroniquement l'identité (par ex. e-ID, permis de conduire, pièce de légitimation de collaborateur ou carte d'étudiant numériques)?

[1] Les cantons de Glaris et Vaud ont chacun soumis deux prises de position. Dans le rapport, elles ont été résumées en une voix par canton.

2 Liste des participants

La liste des cantons, partis politiques, organisations, hautes écoles et entreprises ayant participé à la consultation et leur abréviation se trouve en annexe.

3 Remarques générales

3.1 Processus et document de travail concernant le projet d'identité électronique (e-ID)

La marche à suivre choisie par l'Office fédéral de la justice, comprenant l'élaboration d'un document de travail concernant le projet d'identité électronique e-ID et une consultation publique, a été bien accueillie. Près de la moitié (26) a émis un avis positif au sujet de la démarche ou du contenu du document de travail. Le projet d'avoir, de prime abord, demandé l'avis du public, et donc d'avoir inclus un plus grand cercle d'acteurs dans l'élaboration, a été applaudi. Certains participants ont exprimé le souhait d'avoir la possibilité de prendre part activement aux prochaines étapes.

3.2 Niveau d'ambition

Presque tous les participants ayant exprimé une opinion au sujet du niveau d'ambition (29 sur 31) ont mentionné le niveau d'ambition 3 comme objectif final. Pour n'en citer qu'un, *digitalswitzerland* le justifie ainsi: le plus grand bénéfice, au sens d'une plus-value tant macroéconomique que microéconomique, serait l'établissement d'une structure numérique de confiance, sûre et extensible.

Une progression, du niveau d'ambition 1 au 2 puis au 3, est tout à fait envisageable pour certains participants. Les *vert'libéraux* et *LU* entérinent une progression si cela était favorable à la rapidité d'exécution.

CloudTrust se prononce en faveur d'un niveau d'ambition 2 en citant le manque d'expérience dans le domaine en Suisse; *FR* se prononce en faveur d'un niveau d'ambition 1.

3.3 Approche technologique

Une majorité des participants (31) considère le concept d'identité souveraine (SSI) comme la meilleure solution pour répondre aux exigences de valeurs et de fonctions. C'est la technologie la plus mentionnée des préférences citées (31 sur 38). Pour *BFH* et *Vereign*, c'est même la seule solution possible. *VD (DGS)* et *Switch* ne voient pas la nouveauté de la technologie comme un problème car elle aura gagné une certaine maturité d'ici à une possible mise en service. *esatus* retient que l'utilisateur a une plus grande responsabilité avec l'identité souveraine (SSI): avec l'identité souveraine, l'utilisateur a le contrôle et la responsabilité; ils doivent le comprendre et s'y habituer. *procivis* recommande de convaincre les acteurs principaux des avantages de l'identité souveraine grâce à une stratégie suivie d'information et de formation. *GE* souligne « l'impératif d'une communication large en vue d'une sensibilisation et d'acculturation de la population lors de la mise en place de ce système. »

L'implémentation grâce une infrastructure à clef publique (PKI) a été mentionnée quelques fois, mais seuls *k§rm,* la *FSA* et *swimag* l'ont citée comme application privilégiée.

Pour la *Société Numérique,* l'utilisation d'une infrastructure à clef publique est envisageable comme technologie de transition vers l'identité souveraine.

Une e-ID rendue possible grâce à un fournisseur d'identité (IdP) a été mentionnée comme solution privilégiée par *AG*, *FR* et *GL.* Cette solution a cependant été jugée « non viable à long terme » par d'autres participants et il a été largement reconnu que cette approche ne pourrait pas remplir les exigences exprimées dans la motion. Pour *GE*, « en attendant le projet de base légale fédérale, il doit en effet être possible de collaborer de façon concrète dans notre système fédéral, tant horizontalement que verticalement [et] une e-ID officielle doit [...] répondre aux trois exigences principales suivantes: accessibilité, sécurité, souveraineté. »

Vingt-deux participants n'ont dit privilegier aucune technologie.

À la question de savoir s'il faudrait, pour la sécurité, basculer sur une utilisation d'un hard token (appareil ou boîtier pour la conservation de clefs numériques privées), *BE, BL, DIDAS, FR, Procivis, Sicpa, Swisscom* et *ZH* ont clairement répondu non et ce au profit de la facilité d'utilisation. Pour la *Société Numérique*, les *VERT-E-S* et *Threema* un hard token est quasi indispensable à une e-ID sécurisée.

Indépendamment de l'application, le *Parti Pirate Suisse* demande la portabilité des données d'un appareil à l'autre.

4 Prise de position par rapport aux questions principales du document de travail

4.1 Exigences principales pour l'e-ID comme moyen d'identification numérique

Les motions demandaient notamment l'établissement de l'e-ID par l'État, proposition qui n'a rencontré aucune opposition. Plus de la moitié des participants (35) ont applaudi la demande. Vingt-six participants se sont exprimés de manière positive par rapport à une mise en service par l'État des systèmes nécessaires.

La facilité d'utilisation est l'exigence la plus souvent mentionnée (41). Une vaste majorité a souhaité une solution conviviale et facile d'utilisation. Plusieurs participants (28) ont indiqué que la première étape (d'une utilisation conviviale) est une prise en main facile, l'*UVS* décrit la chose, par exemple, de la manière suivante: l'e-ID ne doit pas présenter de trop grands obstacles pour l'utilisateur et la prise en main et le renouvellement doivent être simples et rapides. L'accessibilité aux personnes handicapées demandée par *BE*, *esatus*, *GE, SDA, swimag* et *Swico* relève aussi de cet aspect.

Le sujet de la protection des données et de la sphère privée se trouve au centre des préoccupations du public et va, à l'avenir, gagner en importance écrit *economiesuisse*. Dans le même sens, une grande majorité (37) exige une solution transparente, mais qui présente un haut degré de protection des données. La protection de la vie privée dès la conception (35) et la maîtrise des données par l'utilisateur (34) ont aussi été mentionnées par une majorité. De même, la minimisation des données a été citée par la moitié de participants (31). *DuoKey* met en avant l'importance de la preuve à divulgation nulle de connaissance (Zero-Knowledge-Proofs).

L'enregistrement des données décentralisé, ou architecture décentralisée, demandé dans les motions, a été jugé souhaitable par 21 participants. Cet aspect a cependant été mentionné moins souvent que les principes fondamentaux énumérés plus haut.

Afin d'améliorer la confiance en l'e-ID, la majorité (35) demande un haut degré de sécurité de l'e-ID et du système y afférant. Pour un grand nombre (24), l'intégrité et la valeur probante de l'e-ID doivent être assurées. *AG* remarque qu'en outre, en cas de perte d'intégrité ou d'attaque

du système vecteur, l'utilisateur de l'e-ID doit pouvoir révoquer la validité à tout moment. D'autres (6) remarquent qu'une révocation doit être possible.

En ce qui concerne la mise en œuvre, plus de la moitié (33) s'exprime en faveur d'un système se basant sur les normes internationales et avec des interfaces ouvertes. *CloudTrust*, *HIN* et *Swico* demandent une mise en œuvre sans le cadre réglementaire « Swiss finish ». Dix participants se sont prononcés pour une utilisation d'un software open source ou d'un développement comme un software open source. Afin de protéger l'investissement de la part des cantons, certains participants (6) demandent une compatibilité avec les systèmes cantonaux existants.

Une bonne diffusion et une intégration dans la vie de tous les jours sont considérées comme des facteurs de succès par la moitié (30). Pour *Switch*, il faut donc que l'utilisation du système aille au-delà des utilisations administratives. Selon *ASB,* une diffusion rapide et accessible doit être au premier plan.

Un bon tiers des participants (17) est d'avis qu'une e-ID et ses utilisations devraient être gratuites tant pour les citoyens que, idéalement, pour les fournisseurs de prestations (partie utilisatrice, vérificateur). Personne n'a proposé que l'utilisateur assume une partie des frais. Pour les *VERT-E-S* et *k§rm*, l'e-ID, et toute l'infrastructure numérique de base de l'État, ne doit en aucun cas être basée sur un modèle économique.

BL et *privatim* remarquent qu'une pondération des critères est indispensable, sans quoi il existe le danger que des exigences incompatibles doivent être mises en place et qu'en fin de compte aucune solution réalisable ne soit disponible.

La compatibilité, voire l'interopérabilité, avec les écosystèmes e-ID numériques européens et internationaux a été demandée par presque deux tiers des participants (39); aucune exigence d'application concrète n'a été mentionnée.

4.2 Cas d'application de l'e-ID (fonctions)

Pour la grande majorité (48), l'e-ID est une carte d'identité numérique dont la fonction principale est la preuve de l'identité. Celle-ci doit pouvoir être utilisée non seulement en ligne (48), mais aussi dans l'environnement analogique (35). La nécessité d'une preuve de l'identité a été mentionnée dans le cadre de la vérification de l'âge (17), de la demande d'un extrait du casier judiciaire (17), de l'ouverture d'un compte en banque (11), de la commande d'une attestation de domicile (6) et de la souscription à un abonnement de téléphone mobile (6).

La possibilité d'utiliser l'e-ID pour accéder aux fonctions de la cyberadministration a été demandée par plus de la moitié (35). Dans ce sens l'e-ID devra faciliter l'accès aux plateformes ou pouvoir être utilisée comme identifiant de connexion. *BE* et *VD (DGS)* veulent éviter que l'utilisateur doive entrer deux identifiants différents pour la cyberadministration et pour le DEP. *CloudTrust* demande une fusion de la SCSE et les règles relatives à l'identité en lien avec le DEP avec la nouvelle loi sur l'e-ID, *ASB* demande une harmonisation de l'e-ID avec les dispositions concernant l'identification de la Convention relative à l'obligation de diligence des banques (CDB). La *FSA* signale d'autres besoins dans le cadre de eJustice 4.0.

Vingt-deux participants se sont prononcés en faveur d'une utilisation de l'e-ID aussi pour les services privés. *KS* demande qu'il ne soit pas possible d'utiliser les identifiants pour des services en ligne de privés. *Switch* considère que la question des identifiants n'incombe pas à l'e-ID.

Une majorité de participants (31) demande que l'e-ID rende possible ou facilite l'utilisation de la signature électronique (qualifiée). Beaucoup souhaitent présenter enfin cette possibilité au

public. Pour *SCTO* et *unimedsuisse*, la signature électronique qualifiée est en haut de la liste des priorités (signature pour consentement, manifestation de volonté).

L'utilisation de l'e-ID pour le vote électronique (5) et la collecte électronique de signatures (5) a été mentionnée quelques fois.

La multitude de cas d'application (présentés ci-dessus) n'ayant aucun lien direct avec l'e-ID et son identification est évidente. Cela est toutefois cohérent à en croire la vision d'un niveau d'ambition 3 décrite plus haut. Le permis de conduire (17), le moyen d'accès à des bâtiments et autres sites (15), le diplôme de formation et les certificats de travail (14), la carte de membre et le badge d'employé (13), les plein pouvoirs et le droit d'accès (4) et d'autres propositions de 37 participants comme preuves de tous types ont été suggérées comme éléments possibles voire nécessaires à la numérisation de la Suisse.

Pour la *ZHAW*, la perspective ne s'arrête pas aux personnes mais s'étend aux organisations et aux choses.

4.3 Utilisation d'une infrastructure nationale de confiance pour les preuves numériques délivrées par l'État et les privés

govtechpodcast pose la question suivant de manière presque philosophique: quels biens publics – analogiques ou numériques, biens, services et infrastructures – doivent mis à disposition par l'État afin de permettre une coexistence libre et en même temps solidaire?

Les prises de position ont offert une réponse possible: l'ampleur des applications souhaitées et l'exigence d'atteindre le niveau d'ambition 3 correspondent au souhait de la majorité (34) de mettre en place une infrastructure permettant une vaste utilisation de preuves numériques de toutes sortes. L'e-ID n'en est qu'une parmi beaucoup d'autres.

Swisscom voit en la tentative de lancer une e-ID nationale, la chance d'établir un écosystème intégral de confiance. Selon *La Poste*, une base commune pour les acteurs du marché réduirait la complexité de l'utilisation et des coûts. Plus de la moitié (32) attend des avantages financiers, une amélioration du rendement et une simplification des processus de la part d'une infrastructure internationale de confiance. L'*ASB*, *ZH* et *ZHR* voient en une infrastructure nationale d'autres avantages qu'une réduction des frais, notamment une diminution du nombre d'erreurs et donc une amélioration de la qualité des données. *SH* note, en rapport avec les usagers d'un écosystème, que les utilisateurs issus du secteur de l'économie pourraient potentiellement profiter beaucoup plus que les particuliers. *NE* voit même un aspect écologique à une infrastructure nationale puisque le trafic routier pourrait être réduit.

Les *CFF* demandent que l'infrastructure de confiance mise à disposition par la Confédération permette une concurrence des logiciels clients novateurs dans l'écosystème des preuves numériques. Pour *ti&m*, un « trust network » offre un haut potentiel d'innovation et de développement pour la Suisse, pays d'accueil des entreprises. Quatorze participants demandent une attitude ouverte vis-à-vis des émetteurs et des vérificateurs. *Switch* réclame une ouverture maximale dans l'application, c'est-à-dire aucune restriction pour les parties utilisatrices (vérificateur) et une ouverture lors de l'inclusion des émetteurs, dans le cadre d'une gouvernance à définir.

Quelques participants (7) remarquent qu'une infrastructure commune rendrait possible des développements ultérieurs efficaces et flexibles. *TG* mentionne en plus la plus grande vitesse de propagation des développements.

Plusieurs participants (18) ont d'ailleurs mentionné que des normes et applications similaires engendrent des avantages, d'autres (16) qu'une infrastructure commune permettrait des économies d'échelle. L'intégration des preuves numériques dans les systèmes préexistants est considérée comme une solution plus facile (13) et on attend un gain général de sécurité (12).

À en croire 24 participants, une infrastructure numérique commune a le potentiel de renforcer la confiance qu'accorde la population au monde numérique. Vingt-cinq participants ont mentionné qu'un point important à cet égard était que cette infrastructure garantit la sécurité juridique à tous les participants si elle est pensée sur le long terme et obéit à des règles de gouvernance globale.

Les questions concernant la distribution des rôles lors de la mise en œuvre de l'infrastructure ne se trouvaient pas au centre du document de travail. Pour la *HSLU*, il est cependant clair qu'il n'incombe pas à la Confédération de développer ou de mettre à disposition tous les éléments mentionnés. Le *Parti Pirate Suisse* exige de réduire à un minimum technique l'infrastructure étatique. L'*USAM* trouve bonne l'idée d'un portefeuille mais ne veut pas d'une solution étatique. Pour *VD*, il est clair que l'État doit prendre en charge le système entier et sa mise en fonction.

5 Remarques sur d'autres aspects

5.1 Législation

Près d'un quart des participants (14) demande une législation neutre du point de vue technologique. *NW* et *OW*, par exemple, l'expliquent de la manière suivante: un cadre légal neutre du point de vue technologique serait approuvé car il faciliterait les développements ultérieurs.

Pour le *PS*, il est important qu'il n'existe aucune obligation directe ou indirecte d'utiliser l'e-ID. *Swico* aimerait donner à la Confédération beaucoup de compétences et réduire à un strict minimum la délégation au niveau cantonal. *swimag* attire l'attention sur l'importance de l'application des lois sur la protection des données existantes.

SDA affirme que la définition antérieure du niveau d'ambition et la préférence pour une solution pourraient créer un précédent pour la législation et qu'une réalisation du système en parallèle à un processus législatif pourrait engendrer des défis relevant du domaine des marchés publics.

5.2 Gouvernance

Le document de travail concernant le projet d'identité électronique (e-ID) ne soulevait pas de questions directes par rapport à la gouvernance. Pour *ZH*, il incombe à la Confédération de prendre en charge la gouvernance. *digitalswitzerland* conseille de ne pas donner à une seule instance tout le contrôle du développement de l'écosystème entier. *DIDAS* demande une séparation nette entre les rôles de l'État et ceux du secteur privé. *esatus* recommande de réfléchir aux questions concernant la gouvernance déjà lors de la phase de conception.

Selon *Switch*, il faudrait faire appel à des organisations du secteur pour la normalisation des données vérifiées (credentials). C'est seulement ainsi que de nombreux cas d'application sans accord bilatéral entre émetteur et vérificateur pourront être mis en place.

Threema demande que les canaux de communication et les procédés de signalement et réparation de failles de sécurité soient définis.

IG eHealth décrit le fait de trouver la gouvernance correcte comme étant un exercice d'équilibre entre une réglementation nécessaire, qui donne confiance et une solution flexible, qui permet la mise en place et le développement dynamique d'écosystèmes privés et publics.

5.3 Risques

Les participants ont attiré l'attention sur de possibles risques: *KS* craint que le transfert général vers le numérique n'engendre un raccourcissement des heures d'ouvertures et une limitation des services publics. Les services publics ne devraient ni être réduits, ni devenir plus chers. L'*usam* considère qu'une participation encore faible des acteurs du secteur privé au projet et le long laps de temps avant l'introduction d'une e-ID sont des risques. *Threema* recommande de ne pas surcharger l'e-ID afin de ne pas la rendre inutilement complexe.

ZH met l'accent sur les exigences en matière de protection des données (notamment l'établissement, l'utilisation de données personnelles) et insiste sur le fait que ce sujet doit encore être discuté. *NEDIK* demande que la priorité soit mise sur la protection des données et du système car, en cas de défaut, il n'y aurait aucun bénéfice pour les utilisateurs; au contraire, cela engendrerait plus de risques.

Pour beaucoup, il est clair qu'il faut encore répondre à de nombreuses questions concernant la technologie SSI, qui est relativement nouvelle. *nets* fait remarquer qu'utiliser la SSI pourrait se révéler une expérience coûteuse.

5.4 Autres précisions

BE trouve important d'inclure toutes les tranches d'âge dans la communication concernant l'e-ID. Par là, on entend non seulement la communication unilatérale, mais aussi les questions et les suggestions sérieuses faites sur les réseaux sociaux auxquelles une réponse devra être apportée et qui devront être prises en compte lorsqu'elles seront jugées raisonnables.

Toujours au sujet de l'âge du public, *SH* et *Sicpa* recommandent d'accorder en plus une attention particulière à la question de l'entrée dans le monde de l'identité numérique pour certaines catégories. D'une part, les smartphones font partie du quotidien des adolescents et d'autre part, il y a encore des questions quant à l'identification grâce à des systèmes biométriques.

DIDAS, *DuoKey* et *SFTI* ont soumis des réponses détaillées aux questions spécifiques à la SSI.

vereign attire l'attention sur la possibilité qu'aurait un utilisateur de retracer son statut avec un audit trail dans une blockchain en ce qui concerne les difficultés qui se posent dans un système décentralisé.

5.5 Suite des opérations

digitalswitzerland, economiesuisse, Sicpa et *Swico* souhaitent l'intégration des différents groupes intéressés dans la suite du processus dans l'objectif d'un pilotage inclusif et afin d'améliorer la confiance. *VD* considère les cantons et les communes comme étant les partenaires principaux devant être associés au processus car ils représentent les prestataires de services en ligne les plus importants qui requièrent la vérification de l'identité. *OBP* considère qu'une formulation transparente des résultats des travaux prenant en compte de tous les partis pertinents est aussi importante.

Il serait important pour *SDA* et *Swico* de pouvoir discuter de la loi sous la forme d'un dialogue parallèle anticipé lors du processus législatif.

Pour les *vert'libéraux*, il est important de développer un écosystème d'e-ID au même rythme que d'autres États.

6 Autres conclusions du débat public

6.1 Enquête de la CSI

Déjà avant la publication du document de travail concernant le projet d'une identité électronique (e-ID), la conférence suisse sur l'informatique (CSI) avait commencé le 27 juillet 2021 à enquêter auprès des autorités et des acteurs économiques en collaboration avec le Verein Schweizerische Städte und Gemeinde-Informatik SSGI.

L'objectif était de se concentrer sur les champs d'application les plus efficaces et acceptés et la coordination entre l'administration de tous les échelons étatiques. Le sondage s'est terminé le 30 septembre 2021.

Les 119 participants au sondage ont tous émis le souhait d'une e-ID uniforme émise par l'État. Les facteurs de réussite suivants ont été mentionnés: un champ d'application large, la fiabilité, un accès facile, peu cher voire gratuit, l'interopérabilité et la compatibilité internationale. La sécurité et la protection des données sont jugées comme des aspects essentiels et la minimisation des données est même considérée comme un élément clef pour l'acceptation de l'e-ID. Les participants au sondage avaient des avis différents concernant la mise en œuvre technique de cette exigence. Plus de la moitié s'est prononcée en faveur d'un service d'e-ID central (IdP) et un tiers préfère une solution décentralisée comme celle visée par l'UE avec l'identité souveraine (SSI).

Concernant les cas d'application, les échanges numériques juridiquement contraignants avec la population et l'économie se trouvaient au centre des réponses de l'administration publique. Ils vont de la signature numérique de documents à la facilitation de l'exercice des droits politiques, la récolte électronique de signatures et le vote électronique, en passant par les démarches faites en ligne sur les portails et auprès des services des autorités. Selon les participants au sondage, la même e-ID doit aussi pouvoir servir au quotidien de moyen de communication sûr entre les entreprises et leurs clients, de méthode rapide et sûre d'exécution de contrat de location et de vente ou encore de preuve de l'âge lors de l'achat d'alcool.

6.2 Conférence

La consultation a été clôturée par une conférence. Des représentants des milieux politiques, de l'économie, des organisations, des cantons, des communes et du Préposé fédéral à la protection des données et à la transparence (PFPDT) se sont exprimés à cette occasion. Les avis communiqués lors de la conférence ont confirmé la direction générale des prises de position déposées dans le cadre de la consultation publique sur le document de travail concernant le projet d'identité électronique (e-ID). L'enregistrement des présentations de la conférence peut être consulté sur le site de l'Office fédéral de la justice.

7 Consultation des prises de position

Les prises de position complètes sur le document de travail concernant l'e-ID de même que le rapport intégral peuvent être consultées sur le site de l'Office fédéral de la justice: *Page d'accueil > État & Citoyen > Projets législatifs en cours > E-ID étatique > Consultation publique sur le Document de travail concernant le projet d'identité électronique (e-ID).*

Verzeichnis der Eingaben
Liste des organismes ayant répondu
Elenco dei partecipanti

Kantone/Cantons/Cantoni

AG	Aargau/Argovie/Argovia, Departement Finanzen und Ressourcen
AI	Appenzell Innerrhoden/Appenzell Rh.-Int. / Appenzello Interno, Ratskanzlei
AR	Appenzell Ausserrhoden/Appenzell Rh.-Ext. / Appenzello Esterno, Informatikstrategie-Kommission
BE	Bern/Berne/Berna, Office d'informatique et d'organisation OIO
BL	Basel-Landschaft/Bâle-Campagne/Basilea-Campagna, Regierungsrat
FR	Freiburg/Fribourg/Friburgo, Chancellerie de l'État de Fribourg
GE	Genf/Genève/Ginevra, Le Conseiller d'État, Département des infrastructures
GL	Glarus/ Glaris / Glarona, Regierungsrat
GL (stva)	Glarus / Glaris / Glarona, Strassenverkehrs- und Schiffahrtsamt
LU	Luzern / Lucerne / Lucerna, Finanzdepartement
NE	Neuenburg / Neuchâtel, Le Conseil d'État
NW	Nidwalden / Nidwald / Nidvaldo, Staatskanzlei
OW	Obwalden / Obwald / Obvaldo, Staatskanzlei
SH	Schaffhausen / Schaffhouse / Sciaffusa, Regierungsrat
TG	Thurgau / Thurgovie / Turgovia, Departement für Inneres und Volkswirtschaft
VD	Waadt / Vaud, Direction générale de la santé DGS
ZH	Zürich / Zurich / Zurigo, Staatskanzlei

Parteien / Partis politiques / Partiti politici

VERT-E-S	Grüne Les Vert·e·s I Verdi
vert'libéraux	Grünliberale glp Vert'libéraux pvl Verdi liberali pvl
Parti Pirate Suisse	Piratenpartei Schweiz Parti Pirate Suisse Partito Pirata Svizzero
PS	Sozialdemokratische Partei der Schweiz SP Parti Socialiste Suisse PS Partito Socialista Svizzero PS

Hochschulen / Hautes écoles

BFH	Berner Fachhochschule, Technik & Informatik, Forschungsgruppe IAM des Instituts IDAS Haute école spécialisée bernoise, technique et informatique, groupe de recherche IAM de l'institut IDAS

HSLU	Hochschule Luzern, Informatik
ZHAW	Zürcher Hochschule für Angewandte Wissenschaften, Expert Group «Blockchain Technology in Interorganisational Collaboration»

Interessierte Organisationen und Unternehmen / Organisations intéressées et entreprises / Organizzationi interessate e imprese

asa	Vereinigung der Strassenverkehrsämter
CloudTrust	CloudTrust SA
DIDAS	Digital Identity and Data Sovereignty Association
La Poste	La Poste Suisse SA
Société Numérique	Société Numérique
digitalswitzerland	digitalswitzerland
DuoKey	DuoKey SA
economiesuisse	Fédération des entreprises suisses
esatus	esatus AG
ZRH	Flughafen Zürich AG
govtechpodcast	govtechpodcast.ch
HIN	Health Info Net AG
eHealth	IG eHealth
k§rm	Kompetenzzentrum Records Management AG
KS	Stiftung für Konsumentenschutz
NEDIK	Netzwerk digitale Ermittlungsunterstützung Internetkriminalität
Nets	Nets A/S, Danemark
OBP	OpenBankingProject.ch
privatim	Conférence des Préposé(e)s suisses à la protection des données
Procivis	Procivis AG
FSA	Fédération Suisse des Avocats
CFF	SBB CFF FSS
SCTO	Swiss Clinical Trial Organisation
Usam	Organisation faîtière de l’économie suisse USAM
Sicpa	Sicpa
UVS	Union des villes suisses
Swico	Association professionnelle pour le secteur des TIC et d’internet
swimag	swimag GmbH
ASB	SwissBanking, Association suisse des banquiers
SDA	Swiss Data Alliance
SFTI	Swiss Fintech Innovations
Swisscom	Swisscom (Suisse) SA

Switch	Switch
Threema	Threema
ti&m	ti&m AG
unimedsuisse	Médecine Universitaire Suisse
Vereign	Vereign AG

Renonciation à une prise de position

– Schweizerischer Arbeitgeberverband (Cf.d prise de position d'economiesuisse)
Union patronale suisse
Unione svizzera degli imprenditori