eCH-0249 – Exigences relatives à un système étatique de gestion des identités (IdMS)

Nom	Exigences relatives à un système étatique de gestion des identités (IdMS)
eCH-nombre	eCH-0249
Catégorie	Document auxiliaire
Stade	Défini
Version	1.0.0
Statut	Approuvé
Date de décision	2022-09-07
Date de publication	2022-12-08
Remplace la version	-
Condition préalable	-
Annexes	-
Langues	Allemand (original), français (traduction)
Auteurs	Groupe spécialisé IAM Annett Laube, Gerhard Hassenstein
Éditeur / distribution	Association eCH, Mainaustrasse 30, case postale, 8034 Zurich T 044 388 74 64, F 044 388 71 80 www.ech.ch / info@ech.ch

Condensé

Le présent document auxiliaire décrit les principales exigences des utilisatrices et utilisateurs ainsi que des services utilisateurs relatives à un système étatique de gestion des identités (IdMS). Pour ce faire, il est procédé au préalable à une comparaison des types possibles de systèmes de gestion des identités (IdMS).

Sommaire

Remarque

En vue d'une meilleure lisibilité et compréhension, seul le genre masculin est utilisé pour la désignation des personnes dans le présent document. Cette formulation couvre également le genre féminin dans ses fonctions respectives.

1 Introduction

1.1 Statut

Approuvé: le document a été approuvé par le Comité d'experts. Il a pouvoir normatif pour le domaine d'utilisation défini dans le domaine de validité donné.

1.2 Champ d'application

La première partie de ce document auxiliaire expose dans les chapitres 1 et 2 les principales différences entre les systèmes de gestion des identités. La seconde partie (à partir du chapitre 3) traite des exigences relatives à l'identité électronique étatique. Les tâches qui en découlent sont celles que l'État (au niveau fédéral, cantonal, voire communal) devrait proposer du point de vue des services utilisateurs et des utilisateurs afin d'offrir une «ancre de confiance» envers un e-ID étatique suisse. Il est entendu dans le présent document que l'e-ID suisse est une E-Identity au sens défini dans le glossaire IAM (eCH-0219 [1]).

Les exigences relatives à un IdMS étatique sont décrites indépendamment de la technologie.

L'identité électronique d'un sujet peut être utilisée pour de nombreuses applications avec des *niveaux de confiance* très différents (voir eCH-0219 [1] ou eCH-0170 [2]). Ce document auxiliaire ne concerne que *l'authentification* [1], qui est ici définie plus avant dans le contexte de l'e-ID suisse:

Log-In (authentification):

L'identité électronique est utilisée par son titulaire à des fins de *log-in* (connexion). Il s'agit pour un sujet de prouver au service en ligne qu'il est bien le titulaire de l'identité électronique prétendue. Il dispose de différents facteurs d'authentification pour en apporter la preuve.

Toute action, que ce soit l'autorisation ou bien l'accès au service en ligne, présuppose invariablement que l'authentification ait réussi.

Cette définition suffit à couvrir les cas d'utilisation les plus courants:

- *Authentification récurrente*: L'utilisateur fait usage de l'identité électronique afin de se connecter à une organisation prestataire de services ou à un écosystème. → Utilisation dans le cadre d'une organisation prestataire de services ou d'un écosystème.
- *Onboarding unique*: L'utilisateur se sert de son identité électronique (créée dans une autre organisation ou un autre écosystème) aux fins de créer une identité électronique dans une organisation prestataire de services ou un écosystème. L'organisation prestataire de services ou l'écosystème peut faire usage de l'identité électronique et des attributs de l'utilisateur. → Acceptation d'une identité électronique externe par une organisation prestataire de services ou un écosystème.

D'autres applications peuvent en principe être envisagées, telles que celles indiquées ci-après. Le

présent document auxiliaire n'entre toutefois pas dans le détail des exigences propres à ces applications:

- **Signature numérique:** Le titulaire d'une identité électronique peut s'en servir afin d'effectuer une déclaration de volonté qui l'engage (signature qualifiée). Outre l'origine (authenticité), une signature numérique implique également l'intégrité des données. Une signature numérique peut être effectuée uniquement avec des procédures asymétriques.
- **Enregistrement de données personnelles**: L'utilisateur ou le titulaire d'une identité électronique doit pouvoir sauvegarder des *données personnelles* et ainsi contrôler l'accès à ces fichiers (p. ex. avec SOLID[1]).
- **Utilisation hors ligne:** Le titulaire d'une identité électronique peut utiliser celle-ci en lieu et place de ses pièces d'identité physiques.
- …

1.3 Classification

La terminologie employée dans le présent document est généralement tirée du document eCH-0219 – «Glossaire IAM» [1], complétée des termes figurant dans l'annexe C. Le document se fonde sur les principes de conception IAM [3] et peut être rangé parmi les «documents auxiliaires complémentaires».

2 Comparaison des systèmes de gestion des identités

Du **point de vue de l'utilisateur**, deux scénarios de classification des IdMS peuvent être envisagés: il s'agit de la *création (ou stipulation)* d'une identité électronique d'une part et de son *utilisation* d'autre part. Les questions, qui en résultent et peuvent servir de critères pour la classification des IdMS, sont les suivantes:

- Qui a délivré mon identité électronique et qui la connaît?
- Qui joue un rôle dans l'utilisation de cette identité électronique?

Les IdMS sont classés ci-dessous sur la base de ces scénarios et critères.

Scénario 1: Création (ou stipulation) d'une identité électronique.

Dans le cas du premier scénario, la création d'une identité, les questions à prendre en compte sont les suivantes:

- Qui gère les informations relatives à mon identité?
- À quel service dois-je m'adresser afin d'obtenir une identité?
- À quel service dois-je m'adresser en cas de modification concernant mon identité?

Il y a deux possibilités à ce sujet:

[1] SOLID (SOcial LInked Data; https://solidproject.org/): vise la décentralisation du World Wide Web. Le mode de fonctionnement des applications web est modifié de manière à ce que l'utilisateur dispose de la maîtrise effective de ses propres données en contrôlant la plateforme.

Processus	Service émetteur d'identité	
		
Création, mutation, suppression de l'identité électronique.	Service d'identité, Organisation prestataire de services	Utilisateur (sujet)

Tableau 1 - Identity master

Dans une première variante, l'identité électronique d'un sujet est prescrite par une instance externe ou bien l'utilisateur crée son identité en concertation avec l'instance externe. Même lorsque l'utilisateur choisit de créer lui-même son identité électronique pour ne la transmettre qu'ensuite, l'instance externe en question prend acte de l'identité électronique et des informations afférentes. Une telle instance externe peut être une organisation prestataire de services (administration ou entreprise par exemple) ou un service prévu à cet effet. À l'opposé, on trouve une approche centrée sur l'utilisateur. Dans ce cas de figure, l'utilisateur crée lui-même son identité électronique, sans qu'aucune autre instance n'en ait connaissance.

Scénario 2: Utilisation d'une identité électronique

Le deuxième scénario à envisager concernant la classification de l'IdMS est le type d'utilisation. Là encore, on distingue deux possibilités.

Processus	Lien avec le service de vérification	
		
Utilisation de l'identité	Lien indirect	Lien direct

Tableau 2 - Type d'utilisation

Lien indirect: **Le sujet ne peut pas utiliser son identité électronique indépendamment d'une instance émettrice d'identité**, car cette dernière est tenue de confirmer en temps utile l'identité électronique du sujet à la partie requérante, après que le sujet s'est authentifié auprès de cette même instance.

Lien direct: Dans le cadre de l'approche ***centrée sur l'utilisateur***, aucun service d'identité n'intervient dans l'utilisation de l'identité électronique. ***Le sujet peut utiliser son identité électronique indépendamment de toute instance émettrice d'identité.*** L'utilisation et la création d'une identité électronique sont donc parfaitement dissociées.

Il existe trois façons de combiner entre eux ces deux scénarios (création et utilisation[2]).

- Détermination par autrui: Tant la création que l'utilisation de l'identité électronique relèvent d'une instance émettrice d'identité.
- Contrôle partiel: L'utilisateur ne peut contrôler que l'utilisation, pas la création.
- Contrôle intégral: Un sujet peut créer, modifier et utiliser lui-même sa propre identité électronique.

Ces combinaisons sont décrites plus en détail dans les chapitres suivants.

2.1 Identité déterminée par autrui

Cette approche classique consiste en une gestion de l'identité électronique d'un sujet par une instance qui lui délivre son identité.

On établit une distinction entre deux instances pouvant créer l'identité électronique d'un sujet. Il s'agit soit de l'organisation prestataire de services elle-même, soit d'un service d'identité spécialisé sur la question.

2.1.1 Identité isolée

Dès lors que l'identité électronique d'un sujet (un client par exemple) est attribuée et gérée individuellement par chaque organisation prestataire de services, on parle bien souvent d'identités **«isolées»**.

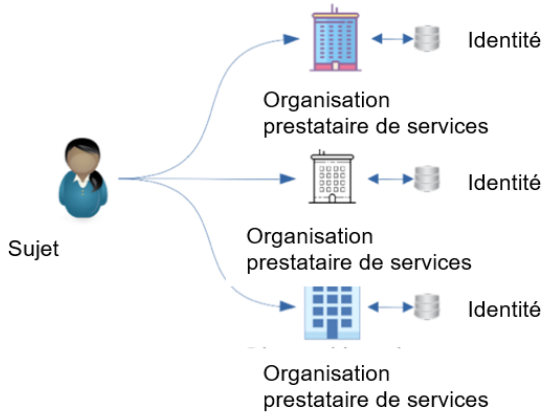

Figure 1: Une identité électronique par organisation prestataire de services (isolée).

Les caractéristiques pouvant être attribuées à cette façon de faire très répandue sont les suivantes:

- l'organisation prestataire de services tient à jour une base de données des utilisateurs (base de données des clients) recensant les données de connexion des sujets dont elle a le contrôle.
- Du point de vue du sujet, la protection de la sphère privée est respectée jusqu'à un certain

[2] La façon dont un utilisateur/titulaire peut prouver qu'il dispose d'une identité électronique (ou en possède) a trait au lien unissant sujet et identité électronique ou à l'utilisation de moyens d'authentification appropriés et n'est tout simplement pas abordée dans ce document.

point, car une autre identité électronique par organisation prestataire de services est possible.

- Un sujet doit gérer une identité spécifique pour chaque organisation prestataire de services (identificateur et moyen d'authentification), ce qui a pour effet d'alourdir la charge de travail à mesure que croît le nombre de relations.
- Toute organisation prestataire de services définit ses propres politiques en matière de sécurité et de protection des données[3], politiques qui peuvent toutes être distinctes (les règles très différentes qui régissent les mots de passe en sont un exemple classique).
- L'organisation prestataire de services est compétente pour la conservation en toute sécurité des informations de ses sujets sur son site. Faute de pouvoir le faire avec succès, elle s'expose à de graves manquements au devoir de confidentialité, comme en attestent certains exemples vécus.
- L'identificateur est spécifique à l'organisation, raison pour laquelle les données d'identité ne sont, en règle générale, pas utilisables ailleurs non plus. L'identité de l'usager dans les transports publics ou la Switch edu-ID dans l'enseignement supérieur en sont des exemples parlants.

2.1.2 Service d'identité spécial

Ceci étant, une organisation prestataire de services peut également associer une identité électronique préexistante, préalablement créée par un service d'identité spécifique, au sujet figurant dans sa base de données des utilisateurs.

L'intérêt étant de pouvoir remédier aux principaux inconvénients (identificateurs spécifiques à l'organisation et conservation des moyens d'authentification) d'une identité isolée. L'organisation prestataire de services ne se charge plus elle-même de l'authentification du sujet, mais délègue au contraire cette étape du processus à une instance externe (service d'identité) en laquelle elle a confiance (d'où le terme *«Relying Party»* ou *«partie de confiance»).* Afin de pouvoir accéder à une ressource de l'organisation prestataire de services, le sujet doit au préalable s'authentifier auprès du **service d'identité externe (IdP),** qui communique alors le résultat de la connexion au service requérant de l'organisation sous une forme appropriée. Le sujet ne dispose d'aucun lien direct avec l'organisation prestataire de services.

[3] Bien que des cadres réglementaires généraux existent comme la LPD [11] ou le RGPD, il arrive fréquemment que ces règles fassent l'objet d'interprétations différentes. Autre facteur rendant impossible l'adoption de directives communes en matière de protection des données, la dimension internationale des services visités.

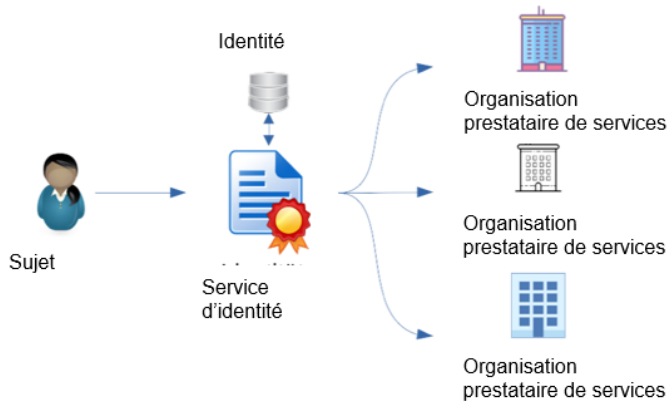

Figure 2: Une identité électronique pour plusieurs organisations prestataires de services (service d'identité externe).

En règle générale, ce service d'identité externe transmettra non seulement une confirmation d'authentification, mais aussi des informations supplémentaires concernant le sujet (attributs) en question, dont il a la compétence dans le cas concret. L'organisation prestataire de services se voit ainsi remettre une copie des informations d'identité et les intègre à ses propres données dans son administration des utilisateurs (base de données des clients). Il lui faut s'assurer, par des moyens appropriés, que les données copiées soient bien mises à jour, pour autant que cela soit pertinent pour l'exploitant du service.

Dans ce modèle, le service d'identité et l'organisation prestataire de services sont des entités organisationnelles distinctes appelées à communiquer entre elles. L'organisation prestataire de services et le service d'identité font partie d'une fédération d'identité. La communication passe par des protocoles courants tels que SAML [4], OAuth 2.0 [5] et OpenID Connect [6]. Une pratique qui s'est intensifiée avec l'émergence des réseaux sociaux tels que Facebook, Google, Twitter... Facebook et Google, par exemple, correspondent au modèle caractéristique d'un service d'identité externe. Mais l'on peut également mentionner à ce stade d'autres fournisseurs d'identité dans le cloud (p. ex. Microsoft), auxquels les entreprises ont de plus en recours afin d'authentifier non seulement leurs clients, mais aussi leurs collaborateurs à l'extérieur.

Les propriétés recensées pour ce type de système d'identité sont les suivantes:

- Le sujet peut utiliser son identité électronique et le moyen d'authentification qui lui est associé pour l'ensemble des organisations (écosystèmes) qui font confiance au service d'identité externe.
- Un SSO sur divers services d'organisations prestataires de services est tout à fait possible et sa mise en place facile.
- L'externalisation de la gestion des identités vers un service d'identité permet aux organisations prestataires de services de réaliser des économies sur les coûts et de s'épargner des efforts.
- Dans la plupart des cas, c'est bien le service d'identité qui détermine les données personnelles collectées pour un sujet.
- Les données personnelles qu'une organisation prestataire de services demandent au service d'identité pêchent souvent par manque de transparence pour le sujet.

- Il n'existe pas de service d'identité unique pour tous les sites web et toutes les applications du quotidien. Un sujet a donc encore besoin de plusieurs services d'identité.
- Les services d'identité sont spécialisés dans l'administration des identités électroniques. Par conséquent, la sécurité des données et la protection des données des identités électroniques revêtent pour eux une importance existentielle. Cela étant, tout service d'identité est doté de politiques de sécurité et de confidentialité qui lui sont propres et compliquent grandement la tâche aux utilisateurs souhaitant obtenir une vue d'ensemble.
- Les grands services d'identité eux-mêmes sont parfois victimes de cybercriminalité. Ils doivent gérer de vastes infrastructures et encourent des coûts élevés afin de garantir la sécurité du stockage, à l'instar d'un modèle isolé.
- Le service d'identité externe est intégré au processus d'authentification entre le sujet et l'organisation. Le service d'identité sait à tout moment quand et où s'est connecté un sujet.
- Le sujet et l'organisation utilisatrice doivent, l'un comme l'autre, avoir confiance en un service d'identité.[4] Le sujet doit pouvoir faire confiance au fait que le service d'identité n'utilise pas les données du sujet de manière abusive et l'organisation utilisatrice doit accorder un certain crédit à la déclaration émanant d'un service d'identité.
- Le nombre de services d'identité étant relativement peu élevé, une situation de monopole et, par voie de conséquence, un effet négatif sur la transparence sont à craindre.
- L'idée qu'un service d'identité puisse retracer et surveiller toutes leurs relations et activités de connexion auprès des organisations n'enchante guère les utilisateurs.
- Les comptes ouverts sur un service d'identité ne peuvent pas être transférés. L'arrêt du fonctionnement d'un service d'identité entraîne un risque de perte de l'identité électronique du sujet ainsi que des données afférentes.

2.2 Identité centrée sur l'utilisateur

Un système de gestion des identités peut également être conçu de manière à ce que le sujet puisse lui-même contrôler l'utilisation de ses informations d'identité. L'avantage est ici qu'il n'y a plus d'implication d'un service d'identité dans le processus d'application (authentification) entre le sujet et l'organisation**. La délivrance de l'identité électronique est dissociée de son utilisation** (y compris dans le temps).

[4] La confiance entre les parties est régie par la définition des devoirs/droits des deux partenaires d'une part, et par la responsabilité applicable en cas de préjudice occasionné par un manquement à un devoir d'autre part. Les règles sont établies par la législation pour les autorités ou par contrat pour les particuliers.

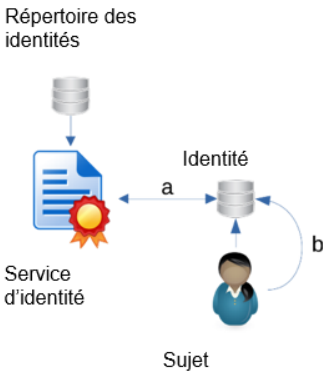

Figure 4: Création d'une identité électronique

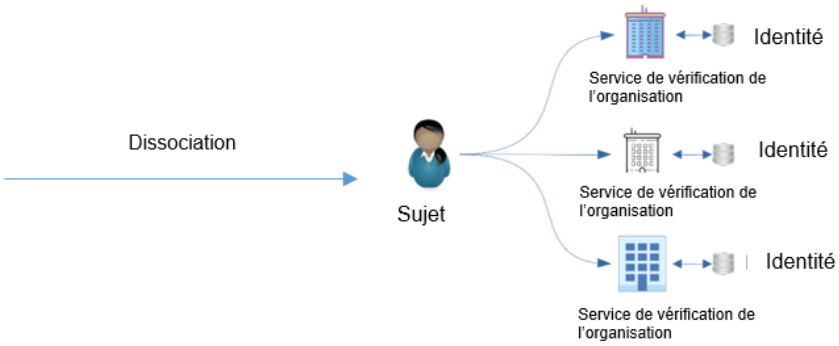

Figure 3: Utilisation de l'identité électronique

L'identité électronique est créée par un service d'identité pour un sujet (a). Cette identité est transmise au sujet sous une certaine forme (comme certificat X.509 ou Verifiable Credential par exemple) à des fins de conservation (chapitre 2.2.1). Le sujet ne peut donc que contrôler l'utilisation de son identité électronique (contrôle partiel). Le sujet dispose d'un lien direct avec le service de vérification de l'organisation. Toutefois, le sujet peut également créer lui-même sa propre identité électronique (b). Dans ce cas de figure, le sujet est en mesure de contrôler la création et l'utilisation de son identité (chapitre 2.2.2).

Outre les avantages majeurs d'une dissociation temporelle lors de l'utilisation d'une identité électronique centrée sur l'utilisateur et du contrôle par le sujet, il est important de tenir compte, entre autres, des points suivants:

- *Agents (agents - delegation):* Qu'un sujet confie son identité électronique à un service spécialement prévu à cet effet (agent) et lui octroie tous les privilèges nécessaires et le principe du contrôle exclusif de sa propre identité électronique n'est alors plus donné. Le sujet doit donc faire pleinement confiance à cet agent.
- *Interopérabilité (interoperability):* Le principe d'interopérabilité [7] prévoit qu'un utilisateur peut à tout moment utiliser, échanger et sécuriser son identité électronique et les attributs afférents (Verifiable Credentials) dans une certaine interopérabilité, en utilisant des normes ouvertes, publiques et gratuites. Une exigence aujourd'hui difficile à satisfaire.
- *Portabilité (portability):* Comment un utilisateur peut-il enregistrer et utiliser son identité électronique sur plusieurs appareils (ordinateur de bureau, ordinateur portable, téléphone portable, tablette)? Cette revendication est tout à fait légitime. Pour ce faire, un utilisateur doit avoir à sa disposition une sauvegarde pour pouvoir la restaurer sur l'autre système. À titre d'alternative, les appareils peuvent également déclencher directement une synchronisation des données qui soit digne de confiance.
- *Confiance (trust):* Un service de vérification doit pouvoir faire confiance aux informations présentées par le sujet. On établit une distinction entre «confiance technique» (p. ex. vérification d'une signature) et «confiance sociale» chez les émetteurs, qui est préparée par une communauté (community) et transmise à ses membres.

Pour des explications complètes concernant les identités électroniques et les IdMS, se reporter à [8].

2.2.1 Identité partiellement contrôlée

L'identité électronique d'un sujet est créée en amont par un service d'identité de manière indépendante (ou avec le concours du sujet) puis **transmise au sujet à des fins de contrôle et de conservation**. L'avantage est ici que le service d'identité n'est désormais actif que lors de la délivrance (et de la mise à jour). L'inconvénient en revanche est que le sujet n'exerce plus guère d'influence sur le processus de création et de transfert. Le sujet doit donc accorder une confiance suffisamment importante à ce service d'identité.
Concernant l'accès à une organisation prestataire de services, le sujet soumet ses informations d'identité au format demandé (sous la forme d'un certificat X.509 ou d'un code QR par exemple). Le service de vérification de l'organisation peut vérifier l'origine et la validité des informations d'identité au terme de la présentation. En fonction de la conception de ces informations d'identité, leur utilisation dans le monde physique est également possible.

En cas de perte de l'identité électronique, le sujet peut s'adresser au service d'identité pour en obtenir le remplacement ou, le cas échéant, la révocation dans un premier temps.

Un exemple typique d'IdMS autocontrôlé est la nPA (nouvelle carte d'identité en République fédérale d'Allemagne) [9]

2.2.2 Identité intégralement contrôlée

Cette approche connue sous le nom de «Self-Issued Identity» ou «Self-sovereign Identity» (SSI) se fait **sans service d'identité central**. Dans cette variante, le sujet **crée et utilise** lui-même son identité électronique. Cette identité électronique peut être reliée, de manière facultative, à un répertoire des identités décentralisé. Par la suite, le sujet peut faire confirmer des attributs (individuellement ou en groupe) par des sources faisant autorité (émetteur). Il faut pour ce faire que le sujet commence par s'authentifier auprès d'un émetteur puis fasse confirmer les propriétés qu'il a lui-même déclarées (déclaration). Le sujet «collecte» ainsi des attributs confirmés (p. ex. *Verifiable Credentials*) relatifs à son identité électronique, qu'il prépare ensuite et présente le cas échéant à un service de vérification (Verifier) au format demandé, comme *Verifiable Presentation* par exemple.

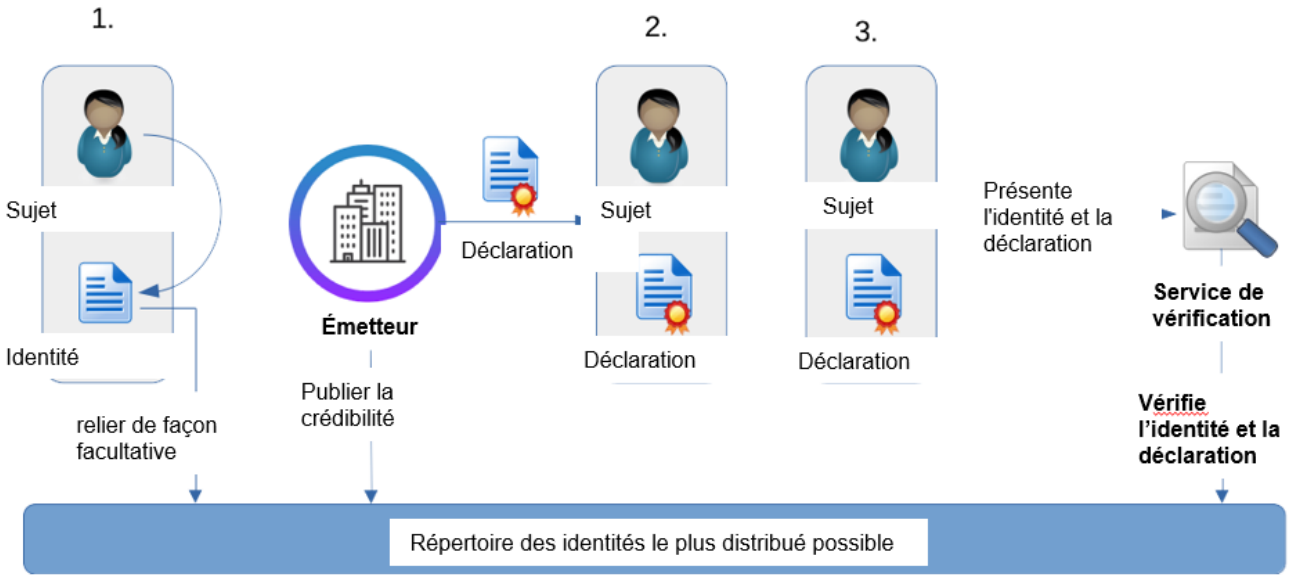

Figure 5: Identité autogérée

Le service de vérification doit pouvoir se convaincre, de quelque manière que ce soit, de l'identité électronique qui lui est présentée et des déclarations afférentes. Différentes approches ont été mises en œuvre à cet effet. Elles vont de la transmission de Verifiable Credentials [10] sous leur forme originale aux Zero Knowledge Proofs (ZKP). Cette variante prévoit que le sujet jouisse de la plus grande autonomie possible, mais assume également une partie importante de responsabilité.

Une «identité autogérée» exige bien plus de responsabilité de la part de l'utilisateur, aucune instance ne pouvant lui venir en aide en cas de problème. Il s'agit notamment de:

- *Récupération (recovery):* Un sujet doit être en mesure d'enregistrer l'identité qu'il s'est créée ainsi que les déclarations qu'il a recueillies dans un environnement sûr et digne de confiance. → Portefeuille numérique (Wallet). Afin de ne pas perdre le principe même du contrôle exclusif de son identité électronique lors d'une sauvegarde (backup), les données personnelles doivent être enregistrées de telle sorte que seul le sujet lui-même (ou des sujets disposant de l'autorisation requise) puisse y accéder. Différentes variantes de solutions ont déjà été suggérées et mises en œuvre à cet égard (systèmes Guardian, Social Key-Recovery, etc.).

2.3 Comparaison des types d'IdMS

Lorsque l'on étudie et compare les différents types d'IdMS à l'aune des scénarios et critères définis au chapitre 2, on obtient l'image suivante:

	Déterminée par autrui	Centré sur l'utilisation	
		Partiellement contrôlé	Intégralement contrôlé
Émetteur de l'identité électronique	Service d'identité	Service d'identité	Sujet
Contrôle via l'identité **électronique**.	Service d'identité	Sujet	Sujet
Contrôle via le moyen d'authentification	Sujet	Sujet	Sujet
Confirmation de l'identité de base	Service d'identité	Service d'identité	L'identité est d'abord auto-déclarée puis confirmée par une source faisant autorité.
Confirmation des attributs	Service d'identité ou autres sources faisant autorité	Service d'identité ou autres sources faisant autorité	Les attributs sont d'abord auto-déclarés puis confirmés ultérieurement par une source faisant autorité.
Authentification	Service d'identité	Service de vérification de l'organisation	Service de vérification de l'organisation
Récupération des informations d'identité en cas de perte	Service d'identité	Service d'identité	Le sujet est lui-même responsable → Enregistrement sécurisé de la clé ou délégation à un tiers.

Tableau 3 – Comparaison des types d'IdMS du point de vue de l'utilisateur.

3 Exigences relatives à un IdMS étatique

L'État et les décideurs politiques doivent se préparer à délivrer des identités électroniques nationales et des documents d'identification, ainsi qu'à poser un cadre technico-juridique (infrastructure de base).

Ces exigences relatives à une infrastructure de base seront par la suite compilées.

- L'État doit mettre en place une infrastructure nationale que tant les particuliers que les autorités pourront utiliser et les parties aux transactions les invoquer. Il est très important, en cas d'introduction de nouvelles technologies, d'imposer une normalisation nationale.
- Les parties aux transactions (personnes et organisations) devraient pouvoir contrôler, de façon bilatérale, les accords, procédures et transmissions de messages.
- Les parties utilisatrices doivent pouvoir faire confiance à l'origine et l'inaltérabilité (intégrité) des données d'identité → **Vérifiabilité technique**.
- La partie utilisatrice doit pouvoir faire confiance à la nature juridiquement contraignante des déclarations faites par le titulaire. Il faut également s'assurer que la déclaration provient bien du titulaire légitime.
- L'État ne doit pas définir ses propres normes de protocole, mais instaurer des solutions aux protocoles existants (reposant de préférence sur des normes internationales). Une solution en matière d'identité prescrite par l'État doit être fondée sur un **concept ouvert** pouvant à tout moment être adapté aux progrès technologiques.
- L'infrastructure doit être compatible avec les solutions d'e-ID dans l'environnement européen, sous réserve que cela soit faisable sans compromettre les niveaux de confiance et d'engagement.

Concernant les données d'identité d'un sujet, l'État devrait respecter les principes suivants:

- Un utilisateur ne peut **pas** se prévaloir d'un quelconque droit à l'**anonymat** dans sa relation à une source faisant autorité. Avant qu'un éditeur (un État d'origine par exemple) ne délivre une déclaration certifiée sous quelque forme que ce soit, il doit identifier l'utilisateur. C'est là le seul moyen pour les services consommateurs de faire confiance aux informations d'identité → L'État joue ainsi le rôle de source faisant autorité de toutes les informations relatives à une identité de base qu'il peut garantir.
- Cela vaut également pour d'autres sources faisant autorité, car elles fournissent des informations le plus souvent basées sur l'identité de base de l'État.[5]
- L'État peut délivrer cette identité de base en tant que certificat x.509 et/ou de Verifiable Credentials. L'important à ce sujet est que les informations d'identité émises par un utilisateur puissent être interprétées par son application et par le destinataire final (service utilisateur).

3.1 Exigences des citoyens[6]

D'une part, l'État doit permettre à ses citoyens une participation sûre et simple[7] à l'univers numérique. Un citoyen, en tant qu'utilisateur d'un e_ID étatique, est d'autre part soumis à certaines exigences par rapport à un service de vérification, destinées à éviter toute utilisation abusive de ses données.

[5] Lorsqu'une source faisant autorité délivre pour un sujet des confirmations sans faire référence à l'identité de base, autrement dit sur la base d'une autre identité électronique, l'utilisation commune de ces confirmations s'en trouve grandement compliquée dans certains cas (Multi-credential verification).

[6] Le terme «citoyen» utilisé dans le présent document désigne tous les habitants et habitantes de Suisse.

[7] La convivialité et la satisfaction de l'utilisateur sont autant de facteurs qui jouent un rôle déterminant en vue d'une utilisation à plus large échelle. L'utilisation de l'e-ID se doit d'être pratique, transparente et néanmoins intelligible.

Outre la convivialité, l'interopérabilité et la portabilité, une solution doit notamment présenter les caractéristiques suivantes:

- **Divulgation sélective** (selective disclosure): L'utilisateur doit avoir la possibilité de ne divulguer, à tout moment, que les informations personnelles (dont les identificateurs) de son choix, à une instance de vérification.
- **Minimisation des données** (data economy): Un service de vérification ne peut exiger d'un utilisateur que les attributs strictement nécessaires à une relation d'affaires (réglés par le point [11]).
- **Anonymat** (anonymity): Dans la grande majorité des cas, un utilisateur ne peut se prévaloir d'un quelconque droit à l'anonymat dans sa relation à un service de vérification. En temps normal, ce dernier veut connaître l'identité électronique de l'utilisateur dont il vérifie les attributs. La technologie employée doit toutefois pouvoir pleinement respecter l'anonymat de l'utilisateur. L'utilisateur doit avoir la possibilité de dissimuler totalement son identité électronique à un service de vérification. Cette exigence n'est possible que si une partie en charge de la vérification est en mesure de se convaincre de certaines informations d'un utilisateur sans en avoir une connaissance concrète. Le respect de l'anonymat d'un utilisateur n'est alors possible qu'avec des procédures prévues spécialement à cet effet (attributs dérivés ou Zero Knowledge Proofs par exemple).
- **Non-associativité** (unlinkability): Lors de l'utilisation de ses informations d'identité, l'utilisateur doit pouvoir partir du principe qu'aucun identifiant sans ambigüité (y compris la clé publique) n'est transmis à plusieurs services de vérification[8] qui leur permettraient de compléter aisément l'identité électronique de l'utilisateur (profilage) ou de transmettre celle-ci à des tiers.
- **Révocation:** L'utilisateur doit, à tout moment, être en mesure de désactiver son identité et d'obtenir la révocation des attributs.

Qui plus est, deux questions, auxquelles un utilisateur ne peut pas répondre lui-même, se posent:

- Un service est-il en droit d'agir en tant que service utilisant l'e-ID? Par exemple, l'assurance «xyz» est-elle autorisée à proposer ses services en tant que tel sur le réseau? Le certificat de serveur web [12] – émis par une instance autorisée – était jusqu'à présent validé par le navigateur. L'éligibilité ne faisait toutefois l'objet d'aucune vérification.
- Quelles sont les informations d'identité (p. ex. nom, sexe, numéro AVS, identificateur sans ambigüité entre RP[9], ...) qui peuvent être collectées par ce service en vue d'établir une relation commerciale avec l'utilisateur[10]?

L'État devrait réglementer les autorisations du service utilisateur de l'e-ID. Il devrait déterminer les informations du sujet auxquelles un service utilisant l'e-ID pourrait accéder, dans quel cas de figure/dans quelles circonstances, et si un service utilisateur dispose d'une autorisation à jouer ce rôle.

[8] Ceci peut être obtenu au moyen d'identificateurs individuels par service utilisateur.

[9] Les identificateurs uniques revêtent une importance particulièrement critique, car ils permettent de regrouper les activités de l'utilisateur auprès de différents services utilisateurs (profilage), ce qui peut également être utilisé de façon abusive à des fins de surveillance (voir aussi: https://epicenter.works/content/orwells-wallet-das-elektronische-identifizierungssystem-der-eu-fuehrt-uns-direkt-in-den).

[10] À ne pas confondre avec le consentement de l'utilisateur (user consent), par lequel il détermine lesquelles parmi ses informations d'identité doivent être partagées avec le service utilisateur.

L'État ne doit toutefois pas se charger lui-même de la mise en œuvre, mais peut déléguer la surveillance et l'attribution à un organisme responsable qui à une meilleure connaissance des services utilisateurs (à un écosystème par exemple).

3.2 Exigences des services utilisateurs

Un changement de paradigme vers des systèmes d'identité centrés sur l'utilisateur et l'établissement de nouvelles technologies (pour autant qu'il s'agisse bien là de l'objectif) doivent être soutenus par l'État, l'utilisateur ainsi que les services qui les utilisent.

Pour un service utilisateur, les exigences principales suivantes résultent de sa fonction:

- **Vérification & autorisation:** Le service utilisateur doit pouvoir vérifier dans les meilleurs délais[11] si les attributs qui lui sont présentés sont bien authentiques et inchangés et s'ils ont bien été délivrés pour cet utilisateur. Qui plus est, il doit pouvoir être vérifié par un service utilisateur afin de s'assurer qu'un éditeur est autorisé ou non à faire une déclaration sur l'utilisateur.
- Un service utilisateur doit en outre pouvoir vérifier les critères suivants:
  - Les informations d'identité présentées sont-elles conformes aux attributs demandés?
  - Les informations d'identité présentées peuvent-elles être interprétées?
  - Peut-on effectuer un contrôle d'accès à partir des informations d'identité présentées?
- **Incontestabilité:** Concernant l'onboarding, le service utilisateur se voit remettre un identificateur lui permettant d'identifier l'utilisateur sans ambigüité et garantissant ainsi l'incontestabilité conformément aux exigences réglementaires, par exemple la LBA [13], dans le cadre des délais de conservation en vigueur.

3.3 Interaction «État – Citoyen – Organisation utilisatrice»

	État	Citoyen	Organisation utilisatrice
Infrastructure de base	Détermine, crée et tient à jour une infrastructure de base.	L'utilisateur utilise l'infrastructure de base existante.	Le service utilisateur utilise l'infrastructure de base existante.
Autorisation	Gère un registre dans lequel sont déposés les organismes responsables / organisations par écosystème.	L'application de l'utilisateur vérifie l'autorisation du service en ligne.	L'organisation obtient l'autorisation d'un organisme responsable / État d'intervenir dans un écosystème donné.
Identité électronique	L'État crée l'identité électronique de l'utilisateur et la lui transmet (centrée sur l'utilisateur).	L'utilisateur contrôle l'utilisation de son identité électronique.	L'organisation vérifie l'identité électronique étatique et peut l'associer à la sienne.

[11] Une vérification dans les meilleurs délais inclut un contrôle de la révocation de l'identité ou d'attributs individuels.

	État	Citoyen	Organisation utilisatrice
Normes	L'État, en tant que fournisseur d'identité, s'accorde avec les organisations utilisatrices concernant les normes.	L'utilisateur bénéficie de la portabilité et de l'interopérabilité grâce aux normes utilisées.	Accepte les normes élaborées en collaboration avec les fournisseurs d'identité.

Tableau 4 – Interaction État – Citoyen – Organisation utilisatrice

4 Bilan

L'État devrait prescrire l'infrastructure de base nécessaire. Cependant, cette dernière n'inclut pas nécessairement de service d'identité national utilisable de façon générale, autrement dit le service d'identité national est utilisé uniquement pour l'émission de l'e-ID, mais pas pour l'authentification (récurrente) ni pour l'onboarding auprès des services utilisateurs.

Aujourd'hui, les systèmes «gérés par autrui» ne sont plus aptes à couvrir toutes les exigences relatives à un IdMS étatique. L'exigence de protection accrue de la vie privée en particulier exclut tout recours à un système «géré par autrui». Une solution d'identité «gérée par autrui» n'a de sens que si la protection de la sphère privée d'un sujet ne joue pas un rôle important ou s'il peut être supposé qu'une confiance dans un service d'identité a été établie. L'un comme l'autre ne sont possibles que dans le cadre d'une organisation (ou d'un écosystème), à l'instar d'un système «Trusted-Third-Party».

Sur l'internet «libre», une solution d'identité «gérée par autrui» se révèle peu adaptée dès lors que la confiance et la protection de la vie privée figurent parmi les exigences imposées. Le nombre de directives de sécurité dont devraient convenir le service d'identité et le service en ligne serait trop élevé, car elles relèvent par principe d'organisations distinctes. Si les réseaux sociaux ont certes recours à ce concept, les objectifs qu'ils poursuivent sont aussi très différents (business cases). L'État devrait se démarquer des réseaux sociaux en délivrant une identité électronique partiellement contrôlée «sérieuse».

5 Exclusion de responsabilité - droits de tiers

Les normes élaborées par l'Association **eCH** et mises gratuitement à la disposition des utilisateurs ainsi que les normes de tiers adoptées, ont seulement valeur de recommandations. L'Association **eCH** ne peut en aucun cas être tenue pour responsable des décisions ou mesures prises par un utilisateur sur la base des documents qu'elle met à disposition. L'utilisateur est tenu d'étudier attentivement les documents avant de les mettre en application et au besoin de procéder aux consultations appropriées. Les normes **eCH** ne remplacent en aucun cas les consultations techniques, organisationnelles ou juridiques appropriées dans un cas concret.

Les documents, méthodes, normes, procédés ou produits référencés dans les normes **eCH** peuvent le cas échéant être protégés par des dispositions légales sur les marques, les droits d'auteur ou les brevets. L'obtention des autorisations nécessaires auprès des personnes ou organisations détentrices des droits relève de la seule responsabilité de l'utilisateur.

Bien que l'Association **eCH** mette tout en œuvre pour assurer la qualité des normes qu'elle publie, elle ne peut fournir aucune assurance ou garantie quant à l'absence d'erreur, l'actualité, l'exhaustivité et l'exactitude des documents et informations mis à disposition. La teneur des normes **eCH** peut être modifiée à tout moment sans préavis.

Toute responsabilité relative à des dommages que l'utilisateur pourrait subir par suite de l'utilisation des normes **eCH** est exclue dans les limites des règlementations applicables.

6 Droits d'auteur

Tout auteur de normes **eCH** en conserve la propriété intellectuelle. Il s'engage toutefois à mettre gratuitement, et pour autant que ce soit possible, la propriété intellectuelle en question ou ses droits à une propriété intellectuelle de tiers à la disposition des groupes de spécialistes respectifs ainsi qu'à l'Association **eCH** pour une utilisation et un développement sans restriction dans le cadre des buts de l'association.

Les normes élaborées par les groupes de spécialistes peuvent, moyennant mention des auteurs **eCH** respectifs, être utilisées, développées et déployées gratuitement et sans restriction.

Les normes **eCH** sont complètement documentées et libres de toute restriction relevant du droit des brevets ou de droits de licence. La documentation correspondante peut être obtenue gratuitement.

Les présentes dispositions s'appliquent exclusivement aux normes élaborées par **eCH**, non aux normes ou produits de tiers auxquels il est fait référence dans les normes **eCH**. Les normes incluront les références appropriées aux droits de tiers.

Annexe A – Références & bibliographie

[1] eCH, «eCH-0219 IAM Glossar, Version 1.0,» 30 November 2018. [Online]. Available: http://ech.ch/de/standards/39940.

[2] eCH, «eCH-0170 Qualitätsmodell zur Authentifizierung von Subjekten, V2.0,» 13 September 2017. [Online]. Available: https://ech.ch/index.php/de/standards/60593.

[3] eCH, «eCH-0107 Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM), Version 3.0,» 07 Februar 2019. [Online]. Available: https://ech.ch/de/standards/60198.

[4] OASIS, «Security Assertion Markup Language (SAML) V2.0 Technical Overview,» 25 March 2008. [Online]. Available: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html.

[5] Internet Engineering Task Force (IETF) , «The OAuth 2.0 Authorization Framework,» 01 October 2012. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc6749.

[6] J. B. M. J. B. d. M. a. C. M. N. Sakimura, «OpenID Connect Core 1.0 incorporating errata set 1,» 8 November 2014. [Online]. Available: https://openid.net/specs/openid-connect-core-1_0.html.

[7] Sovrin Foundation , «Die Grundsätze von SSI,» 16 Dezember 2020. [Online]. Available: https://sovrin.org/wp-content/uploads/Principles-of-SSI-V1.01-German-v01.pdf.

[8] T. Ruff, «The Three Models of Digital Identity Relationships,» 24 April 2018. [Online]. Available: https://medium.com/evernym/the-three-models-of-digital-identity-relationships-ca0727cb5186.

[9] Bundesministerium des Innern, für Bau und Heimat, «Der Personalausweis mit Online-Ausweisfunktion,» 2020. [Online]. Available: https://www.bmi.bund.de/DE/themen/moderne-verwaltung/ausweise-und-paesse/personalausweis/personalausweis-node.html.

[10] W3C, «Verifiable Credentials Data Model v1.1,» 09 Novmbeer 2021. [Online]. Available: https://www.w3.org/TR/vc-data-model/.

[11] «Bundesgesetz über den Datenschutz (DSG),» 1 März 2019. [Online]. Available: https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/de.

[12] CA/Browser Forum, «EV SSL Certificate Guidelines,» [Online]. Available: https://cabforum.org/extended-validation/.

[13] «Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (Geldwäschereigesetz, GwG),» 1 Januar 2022. [Online]. Available: https://www.fedlex.admin.ch/eli/cc/1998/892_892_892/de.

Annexe B – Collaboration & vérification

<Toutes les personnes ayant travaillé sur cette version du document doivent être répertoriées ici.>

Dominic Baumann	BFH
Michael Doujak	Ergon AG
Michael Gerber	
Gerhard Hassenstein	BFH
Christian Heimann	Fedpol
Annett Laube	BFH
Esther Hefti	canton ZH

Annexe C – Abréviations et glossaire

Ce chapitre recense les termes supplémentaires ou modifiés par rapport à l'eCH-0219 – «Glossaire IAM» [1] qui devraient être repris dans une nouvelle version de la norme eCH-0219.

Abréviations

EID	Identité électronique (Electronic Identity en anglais)
IdMS	Système de gestion des identités
IdP	Service d'identité (Identity Provider en anglais)
nPA	Nouvelle carte d'identité
SSI	«Self-Issued Identity» ou «Self-sovereign Identity»
SSO	Single Sign-on (SSO)
ZKP	Zero Knowledge Proof

Glossaire

- **Anonymat:** L'anonymat est le contraire d'une preuve d'identité. Les deux s'excluent mutuellement.
- **Émetteur (Issuer en anglais)**
  Un émetteur atteste des propriétés d'un sujet en tant qu'attributs sous un format standardisé (p. ex. SAML-Assertion, JWS, Verifiable Credential). Un IdP peut intervenir en tant qu'émetteur.
- **Identité de base:** L'identité de base est une identité électronique réglementée par l'État, qui est constituée d'un identificateur sans ambigüité et d'informations personnelles, telles que le nom, la date de naissance et la photo du visage.

- **Système de gestion des identités (IdMS)**
  Synonyme de *système IAM*
- **Titulaire (Holder en anglais):** L'utilisateur (sujet) pour lequel sont émis les justificatifs et qui les conserve sur lui, par exemple dans son portefeuille numérique.
- **Organisation prestataire de services**
  Une organisation qui propose à ses utilisateurs (sujets) un ou plusieurs services techniques en ligne (RP).
- **Service d'identité**
  Un service d'identité gère et délivre des identités. Un service d'identité peut inclure un service d'authentification en ligne et un service de confirmation des attributs.
- **Répertoire des identités**
  Dans un répertoire des identités le plus souvent décentralisé, les identités électroniques et leurs attributs (Verifiable Credentials) peuvent être, à titre facultatif, mis en relation à des fins de vérification de leur existence et de leur crédibilité. Les informations relatives à la désactivation/révocation peuvent également être déposées ici.
- **Écosystème**
  Un écosystème est constitué d'un groupe d'organisations prestataires de services qui utilisent les mêmes identités d'utilisateur, comme les transports publics ou les services de santé par exemple.

Annexe D – Modifications par rapport à la version précédente

Il s'agit de la première version.

Annexe E – Liste des illustrations

Annexe F – Liste des tableaux