



Conception et organisation d'une fédération des systèmes anciens et nouveaux d'identification et de gestion des accès; concept-cadre FIDES: décision

Considérations du Secrétariat général

- 1 En juin 2015, la CDIP a chargé l'agence spécialisée educa.ch de préparer un concept-cadre de fédération des services d'identités pour l'espace suisse de formation. Le mandat découle du point 1.6 du programme de travail 2015–2019 de la CDIP («Education et TIC»): «Permettre l'accès à du matériel pédagogique via le web en fonction des besoins des régions linguistiques et avec la participation des éditions scolaires, notamment en concevant et réalisant une fédération des systèmes anciens et nouveaux d'identification et de gestion des accès».
- 2 L'agence spécialisée educa.ch a préparé le concept-cadre *FIDES. La Fédération des services d'identités pour l'espace suisse de formation*. FIDES est une fédération des services d'identités au service des acteurs de la formation primaire, secondaire I et secondaire II dans tous les cantons suisses. Elle a pour but principal de leur fournir une identité numérique unique pour accéder aux services en ligne dont ils ont besoin. Les autorités cantonales conservent la souveraineté sur les identités numériques qu'elles fournissent à FIDES. Le concept-cadre décrit le fonctionnement de FIDES en traitant des possibilités de pilotage données aux cantons et à la Confédération, des prestations fournies par la fédération et ses participants et des scénarios projetés pour la mise en place. Le concept-cadre prend en considération les approches différentes des systèmes d'identification et de gestion des accès selon les cantons et permet d'échelonner leur participation à la fédération.
- 3 Par le biais de tableaux récapitulatifs, le concept-cadre montre quels seront les coûts générés par la fédération, en distinguant les coûts de mise en place de ceux d'exploitation. Les dépenses des cantons pour réaliser leur connectivité à la fédération ne figurent pas dans ces tableaux. Il est prévu que les cantons participent ensuite au financement de la fédération dès qu'elle sera instituée.
- 4 Dans son rapport «Défis de la numérisation pour la formation et la recherche en Suisse» de juillet 2017, le Conseil fédéral cite FIDES explicitement comme mesure: «La Confédération soutient l'important projet de création d'une Fédération des services d'identité (FIDES), afin que les établissements scolaires des différents niveaux (de l'école maternelle au degré secondaire II) puissent accéder aux médias et aux services numériques à l'échelle suprarégionale et interinstitutionnelle, conformément aux règles en la matière («espace de confiance»)). Concernant l'étendue de la participation de la Confédération, des pourparlers sont en cours avec le SEFRI.
- 5 Le comité consultatif des secrétaires généraux a suivi l'élaboration du concept-cadre, puis la Conférence des secrétaires généraux (CSSG) en a discuté à plusieurs reprises. Les personnes de référence des cantons ont également été invitées à donner leur avis et impliquées dans sa révision. Ce mode de collaboration avec les cantons se poursuivra aux étapes suivantes.
- 6 Lors de sa séance du 7 septembre 2017, le Comité a examiné le dossier et approuvé sans aucune modification le projet de décision à l'attention de l'Assemblée plénière. La question d'une éventuelle participation de Switch continuera d'être étudiée.

- 7 En se fondant sur le concept-cadre présenté, l'agence spécialisée educa.ch va maintenant élaborer un concept détaillé pour la mise en place des structures d'une fédération FIDES, concept qui doit également préciser les points suivants:
 - Organisation du projet relatif à la mise en place de la fédération
 - Garantie d'une participation suffisante de la part des fournisseurs de services en ligne
 - Conditions à remplir par les cantons (par ex. en matière de protection des données)
 - Modalités d'adhésion pour les cantons et les fournisseurs de services en ligne
 - Financement de la mise en place de la fédération
 - Modalités de financement pour la phase d'exploitation de la fédération
- 8 Le concept détaillé de mise en place ainsi que les propositions de financement (budget 2019) doivent être soumis au Comité de la CDIP le 25 janvier 2018.
- 9 Il appartiendra à l'Assemblée plénière de prendre une décision sur la mise en place et le financement.
- 10 Parallèlement à l'élaboration du concept détaillé, les cantons sont invités à définir leur position en ce qui concerne une adhésion à FIDES.

Décision de l'Assemblée plénière

- 1 Le concept-cadre *FIDES. La Fédération des services d'identités pour l'espace suisse de formation* du 18 août 2017 est approuvé.
- 2 L'agence spécialisée educa.ch est chargée de préparer un concept détaillé selon le point 7 des présentes considérations à l'attention du Comité de la CDIP pour sa séance du 25 janvier 2018. Elle impliquera le comité FIDES de la CSSG et le réseau des personnes de référence cantonales dans ce travail.

Zurich, le 26 octobre 2017

Conférence suisse des directeurs cantonaux de l'instruction publique

Au nom de l'Assemblée plénière:

sig.

Susanne Hardmeier
Secrétaire générale

Annexe:

- *FIDES. La Fédération des services d'identités pour l'espace suisse de formation*, concept-cadre du 18 août 2017

Notification:

- Membres de la Conférence

Publication sur le site web de la CDIP

232.3-1.6 ako/bop

FIDES

FÖDERATION VON IDENTITÄTSDIENSTEN
FÉDÉRATION DES SERVICES D'IDENTITÉS

FIDES. La Fédération des services d'identités pour l'espace suisse de formation

Concept-cadre
Version 18.08.2017



TABLE DES MATIÈRES

1	Une fédération des services d'identités pour l'espace suisse de formation	3
1.1	Défis de l'espace de formation numérique	3
1.2	La Fédération FIDES, une contribution à la transformation numérique	4
1.3	Risques possibles en rapport avec la Fédération FIDES	6
2	Mode de fonctionnement de la Fédération FIDES	7
2.1	La Fédération FIDES constitue un espace de confiance	7
2.2	La Fédération FIDES respecte la compétence des cantons en matière de pilotage	7
2.3	Cantons et SP sont les participants à la Fédération FIDES	9
2.4	Services de la Fédération FIDES	9
2.5	Conception technique de la Fédération FIDES	10
3	Mise en place de la Fédération FIDES	11
3.1	Mise en place de la Fédération FIDES	11
3.2	Responsabilités	11
3.3	Adhésion et participation d'un canton à la Fédération FIDES	12
3.4	Coûts de la Fédération FIDES	15
4	Glossaire	17
	Annexe I : Aspects centraux de la Fédération FIDES	18
	Annexe II: Contexte de la Fédération FIDES	26

1 UNE FÉDÉRATION DES SERVICES D'IDENTITÉS POUR L'ESPACE SUISSE DE FORMATION

Une fédération des services d'identités offre la possibilité de prendre en compte et de résoudre des défis croissants auxquels les cantons seront nécessairement confrontés du fait de la numérisation de l'espace de formation. La Fédération FIDES permet d'unifier différents services d'identités du domaine de la formation. Les services d'identités permettent de s'authentifier et d'accéder à des services en ligne dont les utilisateurs finaux (élèves, enseignantes et enseignants et personnels de l'administration) ont besoin. Elle offre en particulier une chance pour les responsables concernés d'influencer l'espace numérique de formation, de le contrôler, de le piloter et de mettre à disposition un accès sécurisé et contrôlable aux services en ligne. Ci-dessous sont présentés les défis, en général, de l'espace numérique de formation ainsi qu'une esquisse des possibilités dont dispose la Fédération pour les résoudre.

1.1 Défis de l'espace de formation numérique

Beaucoup d'aspects de la vie quotidienne ont connu des changements radicaux au cours de ces dernières années, notamment avec les possibilités de la numérisation. L'espace suisse de formation n'y a pas échappé. Ce ne sont pas seulement les possibilités de pilotage qui ont évolué avec ces bouleversements. Aujourd'hui, les responsables de la formation à l'échelon cantonal et fédéral sont plus que jamais appelés à proposer des solutions adaptées aux différents défis. On peut citer par ex. :

- le contrôle des données de l'espace numérique de formation ;
- le pilotage de l'espace numérique de formation de la Suisse aux niveaux cantonal et fédéral ;
- l'instauration d'un climat de confiance dans l'espace numérique de formation de la Suisse ;
- la garantie d'un accès sécurisé aux services en ligne à tous les échelons du système éducatif ;
- le respect de la sécurité juridique pour l'espace numérique de formation de la Suisse.

1.1.1 L'espace numérique de formation en tant qu'espace de données

L'espace numérique de formation de la Suisse est un espace de données au sein duquel des données personnelles sont générées et utilisées pour obtenir l'accès à des services en ligne. Certains cantons possèdent déjà des solutions centralisées ou coordonnées de manière centralisée afin de garantir le contrôle de l'origine de ces données (cf. Annexe II, *Bonnes pratiques concernant les solutions cantonales d'e-ID pour la formation*). La façon dont les données personnelles sont organisées et leur provenance est actuellement très hétérogène. Souvent, ces données sont générées et traitées sans que des standards communs soient pris en compte. En outre, il n'existe pas non plus de règles claires sur la façon de traiter ces données sensibles.

Aujourd'hui des entreprises privées profitent de l'utilisation et de la collecte des données personnelles des utilisateurs. Des prestataires privés proposent de plus en plus des services en ligne avec licences gratuites pour le système éducatif (p. ex. Google Classroom, Microsoft Classroom, etc.). Toutefois, le lieu de stockage et l'utilisation des données générées par l'exploitation de tels produits demeurent en général opaques. En outre, ces services exigent des données personnelles pour l'identification des utilisateurs finaux. Du point de vue de la protection des données, ces contraintes ne vont pas sans poser des problèmes pour les écoles.

1.1.2 Un accès sécurisé aux services en ligne

Il s'agit donc non seulement de les contourner mais surtout de mettre en place à l'échelon national un accès sécurisé aux services en ligne pour tous les échelons du système éducatif. La sécurité résulte notamment de la relation de confiance entre ceux qui proposent un service et ceux qui les utilisent. À cet égard, la personnalisation des données d'utilisation constitue un défi tout particulier. D'une manière générale, le modèle d'affaires des fournisseurs de services (SP) passe par l'utilisation des données personnelles des utilisateurs finaux pour leurs propres besoins. La question devient sensible à partir du moment où les données d'utilisation personnelles sont

revendues à des tiers ou traitées par des tiers sans que les utilisateurs finaux en aient connaissance. En outre, les utilisateurs finaux doivent gérer un grand nombre de comptes et d'identifications, en général pour chaque service utilisé. Les données personnelles sont utilisées différemment par chaque SP au point que les utilisateurs finaux se trouvent confrontés à toutes sortes de conditions très différentes. La base de confiance avec chaque SP doit donc chaque fois être négociée individuellement. Un accès sécurisé aux services en ligne et donc possible, si on peut décider de l'utilisation des données personnelles et si cette décision est réglée et imposée par une relation contractuelle.

1.1.3 Garantir la sécurité du droit

Comme les conditions contractuelles de grands SP internationaux sont en général unilatéralement imposées, il est extrêmement difficile, voire impossible pour les écoles et même pour certains cantons de faire valoir et d'imposer des droits élémentaires. Pour garantir la sécurité du droit dans l'espace numérique de formation de la Suisse et corriger les déséquilibres dans les contrats, il faut négocier des conditions compatibles avec la jurisprudence suisse (p. ex. application du droit suisse, for judiciaire en Suisse, respect des dispositions légales concernant la protection des données, etc.).

1.2 La Fédération FIDES, une contribution à la transformation numérique

La Fédération FIDES permet d'aborder les défis précités de l'espace numérique de formation de la Suisse à l'échelon national. La Fédération donne aux responsables cantonaux de l'instruction les instruments permettant de mettre en œuvre les mesures nécessaires et de faire avancer la collaboration des cantons pour le développement stratégique de l'espace numérique de formation. La Fédération contribue donc de manière substantielle à la constitution de l'espace numérique de formation de la Suisse.

1.2.1 Contrôle des données personnelles

Compte tenu du contrôle de l'espace numérique de formation de la Suisse comme espace de données, la Fédération FIDES présente deux avantages. Elle fixe d'abord des attributs standardisés d'une e-ID nationale pour la formation (cf. Annexe I, *Modèle de l'e-ID nationale pour la formation*). Cette liste d'attributs ne doit pas limiter les cantons dans la configuration de leurs propres e-ID pour la formation mais au contraire les guider pour qu'ils sachent de quels attributs du contexte de la formation les SP ont besoin pour la connexion à leurs services en ligne. Une fois ces attributs standardisés intégrés dans chaque e-ID pour la formation cantonale, il devient beaucoup plus simple tant pour les SP que pour les cantons de relier des services à la Fédération. Ensuite, le recours à des attributs standardisés permet une uniformisation cantonale et nationale des e-ID pour la formation, ce qui permet d'optimiser le contrôle et la protection des données personnelles. Les modalités de transmission de données personnelles sont définies pour tous les participants dans les contrats de participation à la Fédération (cf. Annexe I, *Règlements et contrats*). Le contrat de participant fixe le principe d'option d'adhésion (opt-in) concernant l'utilisation des données (cf. Annexe, *Principes, processus et standards de la Fédération*). La question de savoir comment réglementer exactement l'utilisation des données d'utilisation est encore sujet à discussion.

1.2.2 Possibilités de pilotage pour les cantons

Le Bureau de la Fédération FIDES décide à l'aide d'une liste de critères (cf. Annexe I, *Règlements et contrats*) les SP qui seront admis dans la Fédération. Cette liste est élaborée en commun avec les cantons participants. La discussion sur ces critères est menée entre le Bureau de la Fédération et les représentants cantonaux tout d'abord dans la phase de mise en place puis durant la phase d'exploitation de la Fédération. Les cantons ont également la possibilité d'influencer la Fédération durant ces deux phases par le biais des structures existantes (cf. [chapitre 2](#)).

La Fédération doit promouvoir la coordination intercantonale pour la gestion des identités (IdM) (cf. [chapitre 3.2](#)) afin de garantir la qualité et l'origine des données d'identité.

1.2.3 Confiance et sécurité

La confiance au sein de la Fédération naît à partir de règles et de processus convenus en commun. En outre, il existe une sécurité (au sens de *safety*) résultant de l'utilisation de technologies fixées communément. (cf. Annexe I, *Principes, processus et standards de la Fédération FIDES*).

La Fédération FIDES met en place à l'échelon national des critères, des standards et des règles communs pour la procédure d'identification à des services en ligne (cf. Annexe I, *Principes, processus et standards de la Fédération FIDES*). Tant les SP que les fournisseurs d'identités (IdP) doivent s'y tenir. Ainsi, des conditions identiques pour tous les participants sont créées au sein de la Fédération, ce qui renforce alors la confiance dans l'accès aux services en ligne des SP. Chaque SP qui est admissible pour prendre part à la Fédération conclut des contrats avec celle-ci et s'engage à utiliser les mêmes technologies et processus, de sorte qu'un accès sécurisé aux services en ligne puisse être fourni (voir. Section 2.1).

Grâce aux contrats entre la Fédération FIDES, les SP et les cantons, la sécurité juridique pour les participants est accrue (cf. aussi [chapitre 2.1](#)). L'avantage réside dans le fait que les conditions-cadres sont les mêmes pour tous les participants et qu'elles ne doivent plus être négociées isolément entre les cantons, les communes ou les écoles et les SP. En revanche, ces contrats ne remplacent pas les relations contractuelles entre les écoles, les communes ou les cantons et les SP concernant l'utilisation des services en ligne.

1.2.4 Collaboration

Le fait que les instances du système éducatif fassent front commun au sein de la Fédération FIDES renforce leur position dans les négociations avec les SP. Les standards communs et l'échange d'expériences à l'intérieur de la Fédération aident les cantons à gérer les identités et à mettre à disposition une e-ID pour la formation cantonale de la manière suivante :

- mise à disposition d'un accès personnalisé, sûr et contrôlable aux données et aux services ;
- optimisation du monitoring grâce à une qualité améliorée et à l'intégrité des données numériques ;
- augmentation de la qualité des données d'identité grâce aux attributs standardisés de l'e-ID pour la formation.

Les prestations de la Fédération FIDES présentent une utilité à la fois pour le système éducatif suisse et pour l'espace suisse de formation, et ce de la manière suivante :

- exigences uniformes pour les SP en ce qui concerne la sécurité et la protection des données ;
- position forte dans les négociations avec les SP pour des modèles d'affaires et des prix avantageux ;
- support dans des domaines stratégiques tels que l'intégration de nouvelles prestations, les relations entre fédérations, les développements techniques, l'optimisation de processus administratifs et techniques, la gestion des risques.

La participation à la Fédération FIDES est également avantageuse pour les SP. Les standards communs et les échanges d'expériences sont également adaptés à leurs besoins tandis que les règlements et les contrats de la Fédération leur offrent sécurité et confiance. Pour les SP, le travail de la Fédération présente l'utilité suivante :

- contrôle des accès simple et efficace pour les offres des prestataires grâce à une infrastructure, une organisation, une technique et des standards centralisés ;
- qualité, sécurité et confiance grâce à des identités numériques officiellement contrôlées.

1.3 Risques possibles en rapport avec la Fédération FIDES

La Fédération FIDES fait naître aussi bien des risques directs qui agissent sur la Fédération que des risques indirects en relation avec la Fédération et qui doivent être supportés par tous les participants :

- La coordination requise par la Fédération concernant l'IdM géré par les cantons et les communes ne représente pas pour tous les cantons la même charge de travail (cf. [chapitre 3.3](#)).
- La participation des SP implique leur disponibilité à accepter les conditions-cadres de la Fédération. Certaines conditions (standardisation, attributs pseudonymisés, traitement ultérieur des données d'utilisation) pourraient avoir une influence sur les modèles d'affaires des SP qui pourrait les inciter à ne pas participer à la Fédération.
- Il faut que suffisamment de cantons participent à la Fédération pour que celle-ci puisse être mise en place et exploitée de manière pérenne.
- L'accumulation de données personnelles recèle de manière générale un certain risque de sécurité dont il convient de tenir compte (cf. Annexe I, *Principes, processus et standards de la Fédération FIDES*).
- Les exploitants des solutions IdM répondent de l'intégrité, de la disponibilité et de la validité des e-ID pour la formation. Ils doivent pouvoir garantir que des personnes non autorisées ne pourront en aucun cas faire un mauvais usage des e-ID pour la formation.

2 MODE DE FONCTIONNEMENT DE LA FÉDÉRATION FIDES

La Fédération FIDES prend en compte les responsabilités de la Confédération et des cantons et contribue à la coopération de tous dans l'espace suisse de formation. Elle offre aux membres du système éducatif un accès aux services en ligne simple, d'utilisation aisée et sûr.

2.1 La Fédération FIDES constitue un espace de confiance

Comme expliqué au début, la Fédération FIDES propose un cadre pour la collaboration entre les cantons et les SP. Les membres du système éducatif reçoivent au sein de ce cadre réglementé un accès aux services en ligne et s'engagent à respecter des standards durables pour la gestion et l'utilisation des identités numériques ainsi que pour l'utilisation des données personnelles. Il est ainsi possible de mettre en place un pilotage étatique de l'espace numérique de formation en respectant la protection des données personnelles et une utilisation des services en ligne conformes aux contrats.

Cela dit, la Fédération ne redistribue pas les responsabilités entre les participants de la Fédération. Plutôt, la Fédération crée un espace de confiance entre les IdP des cantons participants et les SP connectés à la Fédération. L'espace de confiance est défini, d'une part, via la connexion des domaines de sécurité des IdP et SP dans lequel l'administration des données d'identité et d'utilisation est contrôlée. D'autre part, via des normes contraignantes et uniformes et des règles pour la procédure d'authentification qui sont introduite par la Fédération.

Il en résulte ainsi pour les différents acteurs les avantages suivants :

- Les cantons définissent quelles données d'identité sont transmises aux SP. De plus ils peuvent s'exprimer sur la façon dont peuvent être traitées les données d'identité et d'utilisation des utilisateurs finaux par les SP.
- Les utilisateurs finaux peuvent se fier au fait que leur identification auprès d'un service en ligne se fait selon les standards et les règles définies et acceptées au sein de la Fédération.
- De leur côté, les SP savent que les utilisateurs finaux qui s'identifient sur leurs services en ligne y sont habilités.

2.2 La Fédération FIDES respecte la compétence des cantons en matière de pilotage

Les mandants de la Fédération FIDES sont les cantons. Ils pilotent celle-ci dans le cadre d'une convention de prestations qui fixe les objectifs, les prestations et les moyens financiers disponibles (cf. Annexe I, *Règlements et contrats*).

Les cantons sont représentés par le Secrétariat général de la CDIP. La forme concrète des relations entre la Confédération et les cantons dans le cadre de la Fédération et la manière dont celles-ci se refléteront dans la convention de prestations doivent encore être précisées. La deuxième partie contractante est l'agence spécialisée educa.ch qui a été proposée comme mandataire pour la mise en place et l'exploitation du Bureau de la Fédération.

Voici une présentation des instances et des structures retenues pour le pilotage de la Fédération :

2.2.1 Assemblée des participants

La structure d'organisation de la Fédération FIDES prévoit des possibilités de consultation pour les participants. Elle fait une claire distinction entre, d'une part, les instances du système éducatif impliquées dans le processus de pilotage de la Fédération et dans les processus d'exploitation pour le développement et la mise en place de solutions organisationnelles et techniques et, d'autre part, les SP dont leur influence se limite au domaine technique.

Au niveau local, les instances du système éducatif participant à la Fédération sont les écoles avec leurs personnels enseignants, leurs personnels administratifs, les élèves ainsi que leurs représentants légaux pour lesquels l'accès aux services en ligne est prévu. Ils sont représentés dans la Fédération par la personne responsable pour l'IdM cantonal dans le domaine éducatif. Cette personne responsable veille à ce que les membres du système éducatif disposent d'une procédure d'identification sûre et sécurisée. Elle connaît les solutions pour que cette exigence soit remplie au niveau scolaire ou au niveau cantonal. En ce qui concerne la participation des écoles à la Fédération, cette personne veille à l'interopérabilité entre les e-ID pour la formation cantonale et les e-ID pour la formation de la Fédération. Elle peut se mettre en réseau avec les autres représentants cantonaux et communiquer de manière transparente avec les SP. Pour cet échange, la Fédération prévoit une assemblée des participants.

2.2.2 Structures de pilotage existantes

La décision de participer à la Fédération FIDES fait partie des mesures cantonales pour la transformation numérique du système scolaire cantonal. Une fois celle-ci prise, elle est mise en œuvre par le spécialiste compétent pour l'IdM cantonal.

Cette décision soulève toutefois aussi des questions concernant une stratégie commune des cantons pour la transformation numérique du système éducatif suisse. Ces débats doivent être menés par les responsables de la politique de la formation. Ils sont transmis aux structures de la CDIP où ils sont régulièrement mis à l'ordre du jour des instances concernées (nous pensons à la CSSG).

Ceci dit, la Fédération n'est pas une mesure portée par les seuls cantons, mais en commun avec la Confédération. Elle repose sur la loi sur la coopération dans l'espace suisse de formation¹ et relève du domaine de compétence du « Comité de coordination Numérisation de l'éducation (CC N)² ». En ce qui concerne la Fédération, ce comité constitue le niveau national dans lequel la Confédération et les cantons discutent ensemble des questions de pilotage de la Fédération. Le CC N préparera à l'intention des décideurs de la politique de formation de la Confédération (SEFRI) et des cantons (CDIP) la formulation et l'attribution de la convention de prestations pour la Fédération, le contrôle de sa mise en œuvre ainsi que les décisions sur le développement ultérieur de la Fédération. Il est prévu que le CC N reçoive un appui conséquent du Bureau de la Fédération. Le CC N n'aura qu'à valider les propositions du Bureau et les préparer pour adoption par les décideurs de la Confédération et des cantons.

2.2.3 Bureau de la Fédération FIDES

Le Bureau de la Fédération FIDES garantit les processus de pilotage et d'exploitation de la Fédération. Selon la convention de prestations, il veille à ce que les objectifs stratégiques du processus de pilotage de la Fédération soient mis en œuvre par les services de la Fédération. Il définit l'organisation concrète dans des règlements et des contrats, définit les rôles, fonctions, droits et devoirs de tous les participants à la Fédération et spécifie les services techniques de la Fédération (cf. Annexe I, *Règlements et contrats*).

Le Bureau mandate et dirige le Service technique de la Fédération. Ce dernier met à disposition l'infrastructure et assure l'exploitation technique.

¹ L'Assemblée fédérale de la Confédération suisse (2016). *Loi fédérale sur la coopération entre la Confédération et les cantons dans l'espace suisse de formation du 30 septembre 2016*. www.admin.ch/opc/fr/classified-compilation/20152556/201702010000/410.2.pdf (07.01.2017)

² Confédération suisse, CDIP (2016). *Mandat du Comité de coordination Numérisation de l'éducation (CC N)*. edudoc.ch/record/124948/files/mandat-koa-digi_f.pdf (07.01.2017)

2.3 Cantons et SP sont les participants à la Fédération FIDES

Les participants de la Fédération FIDES sont, d'une part, les cantons et d'autre part, les SP. D'un point de vue technique, ils ont pour tâche de permettre aux titulaires d'une e-ID pour la formation d'accéder à des services en ligne. La Fédération apporte son soutien en fédérant les exigences juridiques, organisationnelles et techniques dans des contrats et règlements (cf. Annexe I, *Règlements et contrats*). L'acceptation de ces dernières est la condition pour adhérer à la Fédération. Les cantons et les SP doivent le confirmer par la signature d'un contrat spécifiant les modalités de leur participation.

2.3.1 Cantons

Les cantons reconnaissent dans leur contrat de participation leur responsabilité pour l'e-ID pour la formation que les membres de leurs écoles utilisent. La forme contractuelle instaure une obligation afin que les cantons remplissent leur rôle dans le processus d'identification aux services en ligne. En acceptant cette obligation, ils se portent garants du fonctionnement, du contenu et de la qualité de l'e-ID pour la formation. Elle comporte les points suivants :

- seuls les membres du système éducatif possèdent une e-ID pour la formation ;
- chaque e-ID pour la formation est attribuée à une seule et unique personne et les attributs qu'elle contient correspondent aux exigences du modèle commun de l'e-ID pour la formation nationale (cf. Annexe I, *Modèle de l'e-ID nationale pour la formation*) ;
- l'e-ID pour la formation est sous la responsabilité des cantons dans le cadre d'un IdM pertinent ;
- que se loguer avec l'e-ID pour la formation est à tout moment possible ;
- les identités numériques sont suffisamment protégées contre un accès non autorisé.

En contrepartie, les cantons reçoivent comme participants à la Fédération un droit d'intervention dans les processus organisationnels et les standards techniques. En leur qualité d'associés à l'espace de confiance, ils peuvent élaborer avec le Bureau de la Fédération des propositions de développement de la Fédération qui seront soumises au CC N et aux mandants.

2.3.2 Fournisseurs de service (Service Provider SP)

Des critères de participation s'appliquent également aux SP (cf. [chapitre 1.2.2](#)). Le contrat de participants contient les exigences juridiques, organisationnelles et techniques requises. La Fédération FIDES ne résout pas la question des possibilités d'utilisations pédagogiques et n'est donc pas l'objet du contrat de participant.

Les SP reçoivent un droit de consultation à l'assemblée des participants dès le moment où ils font partie de la fédération. Ce droit porte sur le développement et la mise en place de solutions techniques.

2.4 Services de la Fédération FIDES

La Fédération FIDES fournit à ses participants des prestations de services dans les domaines de l'organisation et de la technique. Ces deux domaines bénéficient de services d'information et de communication.

Les services d'organisation de la Fédération FIDES garantissent la collaboration des participants. Ils comportent notamment :

- la mise en œuvre de la stratégie de Fédération et le suivi des règlements ;
- l'innovation et le développement de l'espace numérique de formation de la Suisse ;
- la direction de la Fédération ;
- l'admission de nouveaux participants dans la Fédération ;
- la communication et la mise en réseau.

Les services techniques de la Fédération concernent le raccordement de nouveau IdP et de nouveaux services en ligne ainsi que la sécurité de l'exploitation technique. Ils sont fournis par le Service technique qui offre son aide aux participants et les conseille dans la planification et la mise en œuvre de leurs projets. L'assistance technique se fait via le site web de la Fédération dans lequel les participants ont accès à tous les documents et règlements concernant la Fédération. C'est sur ce site également que sont publiés les listes des participants et des métadonnées leur appartenant.

2.5 Conception technique de la Fédération FIDES

D'un point de vue technique, la Fédération FIDES suit la solution de SWITCH qui a fait ses preuves dans le domaine de la formation tertiaire. Pour le développement de l'architecture technique, pour le choix des technologies et pour la mise en œuvre, la Fédération recourra à des standards existants (standards eCH et autres) et à des exemples de bonnes pratiques en Suisse (SWITCH, SuisseID, Fédération suisse d'identités dans le domaine e-Gov) et en Europe (Danemark, Estonie, Pays-Bas, Suède) (cf. Annexe II, *Projets et bonnes pratiques de fédérations de services d'identités au plan national ; Bonnes pratiques de fédérations des services d'identités du domaine scolaire de pays européens*).

Le processus-clé de la Fédération réside dans l'authentification par un IdP des utilisateurs finaux avec leurs données d'identification personnelle afin de leur donner accès aux services en ligne des SP. Dans la Fédération, l'authentification n'est plus faite côté SP, mais via l'IdP qui assure la vérification de l'identité de l'utilisateur final. Sur requête du service en ligne, l'IdP transmet au SP les attributs nécessaires sous forme d'un *certificat* numérique d'autorisation. Ce *certificat* transmet au service en ligne les attributs nécessaires pour l'autorisation mais pas l'identité complète de l'utilisateur final. L'utilisateur final apparaît donc au SP sous un pseudonyme, ce qui permet d'optimiser la protection des données.

La mise en œuvre technique de cette procédure exige que les attributs d'une e-ID pour la formation à transmettre aient été standardisés. Au plan technique, les conventions entre l'IdP et le SP sont échangées par le service central téléchargement de métadonnées (*Metadata Download*). Les attributs de l'e-ID pour la formation sont transmis aux SP via le navigateur de l'utilisateur final (cf. Annexe I, *Modèle de l'e-ID nationale pour la formation*).

3 MISE EN PLACE DE LA FÉDÉRATION FIDES

Ce chapitre présente divers aspects de la mise en œuvre de la Fédération FIDES. Tout d'abord, un scénario pour le déroulement de la mise en place de la Fédération est présenté. Celui-ci a été choisi comme étant le plus vraisemblable après évaluation de la situation actuelle. Puis sont décrites les responsabilités des acteurs qui doivent être prises en compte lors de la mise en place de la Fédération. Enfin sont présentés les coûts d'une adhésion à la Fédération pour les cantons ainsi que les coûts du Bureau et leur financement.

3.1 Mise en place de la Fédération FIDES

La mise en place de la Fédération FIDES suppose une décision positive de l'assemblée plénière de la CDIP et se fonde sur les bases conceptionnelles actuelles. Sur la base de ces hypothèses, les étapes suivantes sont prévues :

- Les cantons mandatent educa.ch, dans le cadre d'une convention de prestations, pour créer et mettre en place la Fédération ;
- Le Bureau de la Fédération est constitué et décide de l'organisation du Service technique ;
- Le Bureau élabore les documents contractuels nécessaires pour la participation et conclut des contrats avec les cantons participants ;
- Les cantons participants vérifient la compatibilité de leur IdM avec la Fédération en vue de leur participation et, le cas échéant, l'adaptent aux exigences de la Fédération avec l'aide du Bureau ;
- Le Bureau organise et met en place les processus-clés de la Fédération, acquiert, fait développer ou développe lui-même les logiciels nécessaires ;
- Le Bureau crée une plate-forme test pour les IdP et les SP afin que ceux-ci puissent vérifier que les différents systèmes techniques fonctionnent ensemble ;
- Avec l'aide du Service technique de la Fédération, les cantons participants développent les interfaces nécessaires ;
- Le Bureau négocie avec les SP leur adhésion à la Fédération et élabore ou conclut avec eux les contrats nécessaires ;
- Les SP adaptent leurs systèmes aux standards de la Fédération, avec l'aide du Service technique ;
- Le Bureau exploite la Fédération avec les cantons participants et les SP.

Ce scénario est sujet à des variantes en fonction de la disposition des différents cantons et/ou des SP à adhérer à la Fédération. Cette disposition a une forte incidence sur les besoins en personnel de la Fédération (cf. Annexe I, *Scénarios pour la mise en place de la Fédération FIDES*).

3.2 Responsabilités

Ce chapitre décrit les responsabilités à prendre en considération et les acteurs qui doivent les assumer pendant la mise en place et l'exploitation de la Fédération.

3.2.1 Mandants

- La CDIP rédige une convention de prestations pour la mise en place et l'exploitation de la Fédération FIDES.
- Le financement du Bureau de la Fédération sera discuté avec les mandants. Ceux-ci doivent garantir que les moyens financiers sont disponibles afin d'assurer sa mise en place et son exploitation.

- Les mandants doivent décider des options de mise en œuvre décrites dans l'Annexe I : *Scénarios pour la mise en place de la Fédération FIDES*.

3.2.2 Cantons

- Les cantons sont chacun responsables de leur propre IdM.
- L'IdM d'un canton peut aussi bien être organisé de manière centralisée ou non centralisée. Ce qui est décisif, c'est que le canton puisse transmettre à la Fédération FIDES les informations et contacts nécessaires pour le raccordement de son propre IdP. Les cantons sont toutefois libres quant à la manière dont ils s'organisent (les dépenses éventuelles sont décrites sous le [chapitre 3.3](#)).
- Les cantons examinent avec leurs écoles les services en ligne dont ils ont besoin et définissent ceux qui seront mis à disposition par la Fédération.
- Les cantons coordonnent l'adaptation des interfaces de leurs IdP à l'interface de la Fédération.

3.2.3 Bureau de la Fédération

- Le Bureau est compétent pour le Service technique et pour les processus requis pour la mise en place et l'exploitation ultérieure de la Fédération FIDES.
- Il prête son assistance pour le raccordement des IdP et des SP à la Fédération et est l'interlocuteur des cantons pour le développement futur de la Fédération et pour les problèmes d'exploitation.
- Le Bureau est compétent pour les contrats avec les cantons et les SP ainsi que pour les éventuelles négociations visant à une connexion entre fédérations.
- Le Bureau coordonne avec les cantons participants la discussion sur les critères d'admission des SP dans la Fédération.

3.3 Adhésion et participation d'un canton à la Fédération FIDES

Le concept de la Fédération FIDES prévoit en principe que les cantons adaptent eux-mêmes leur IdM aux exigences de la Fédération et assument les coûts de cette adaptation. Pour soutenir les cantons, un aperçu des éventuelles dépenses à prévoir est proposé. Cet aperçu demeure général car les conditions varient d'un canton à l'autre. Le modèle a été validé lors d'entretiens avec cinq personnes de référence issues des cantons. En outre, les hypothèses considérées ont été comparées avec des projets IdM en cours ou déjà terminés dans leurs cantons. Le modèle a été dans l'ensemble confirmé et seuls quelques ajouts ont dû être encore pris en considération.

3.3.1 Bases décisionnelles

Avant de décider d'adhérer à la Fédération FIDES, les cantons devront procéder à une clarification interne des charges qu'une adhésion entraînera pour eux.

L'adhésion devrait se baser sur les stratégies de formation et contribuer à une utilisation sécurisée des services en ligne dans l'enseignement, les écoles et l'administration scolaire. Pour cela, la législation cantonale doit permettre de mettre en place un IdM coordonné par le canton. À cet égard, la répartition des tâches entre le canton et les communes jouera un rôle décisif dans la coordination. Pour FIDES, il demeure toutefois primordial que le canton assure la coordination de l'IdM. De l'avis des personnes de référence des cantons, cette coordination (ou l'élaboration de ses bases conceptuelles) constituera la principale charge de travail. Il faudra également vérifier s'il existe un cadre juridique portant sur l'utilisation d'un e-ID pour la formation. Le délégué cantonal à la protection des données devra être associé à ces démarches.

Certains cantons ont déjà une solution IdM ou ont tout au moins déjà élaboré une stratégie de mise en place (cf. Annexe II : Bonnes pratiques au niveau cantonal). Il n'est cependant pas décisif pour la fédération de savoir si l'organisation prévue par le canton est centralisée ou non.

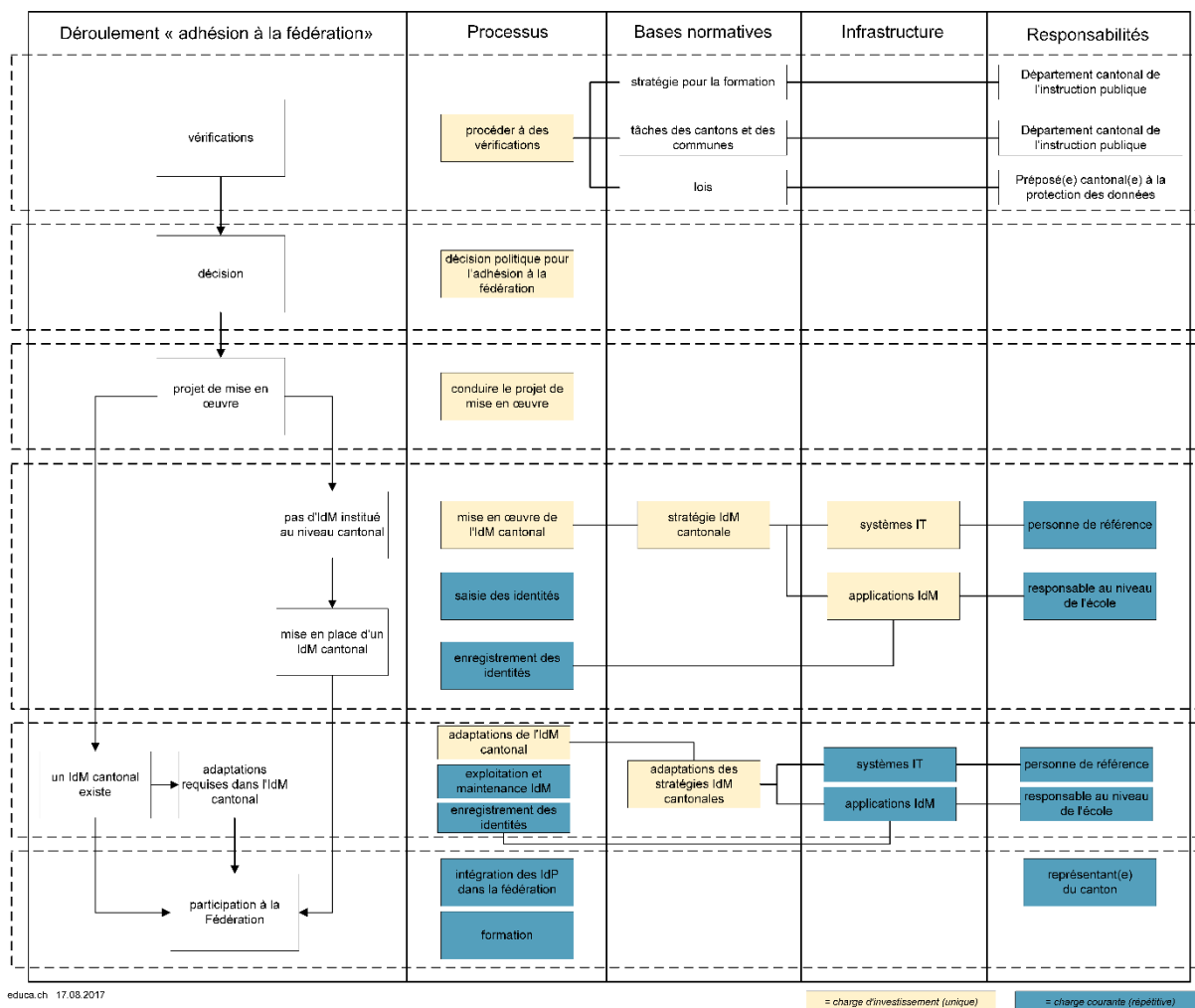


Figure 1 : Adhésion et participation d'un canton à la Fédération FIDES

Ce qui est donc déterminant pour l'adhésion, c'est que le canton crée les bases de sa propre coordination de l'IdM. Un IdM répond aux exigences de FIDES lorsque le canton est en mesure d'assumer la responsabilité de la mise à disposition des e-ID pour la formation, qu'il assure lui-même la coordination de l'IdM et qu'il est en mesure d'établir une liste des services d'identité (IdP) utilisés dans l'IdM. (cf. Annexe II : 2. Bonnes pratiques concernant les solutions cantonales d'e-ID pour la formation)

Au-delà des clarifications d'ordre stratégique, juridique et organisationnel, le canton doit évaluer si la fédération offre une utilité pour lui.

Résultats possibles :

- Le canton constate que son adhésion à la Fédération FIDES présente pour lui une utilité, qu'il possède les bases nécessaires à cette fin ou qu'il prévoit de les préparer.
- Le canton ne voit pas d'utilité à adhérer à la Fédération FIDES ou n'a pas les moyens pour mettre à disposition les bases nécessaires.

3.3.2 Décision

La décision de participer à la fédération est une décision politique prise dans les structures existant dans le canton. Il englobe au moins trois décisions singulières :

- La décision principale de participer à la Fédération FIDES,
- Le moment prévu pour adhérer à la Fédération FIDES,
- Les mesures à entreprendre pour participer à la Fédération FIDES et préparer l'adhésion.

3.3.3 Projet de mise en œuvre

Si le canton se prononce pour l'adhésion, il procède à un projet de mise en œuvre de celle-ci. Son ampleur dépend du résultat des clarifications faites. L'étendue du projet de mise en œuvre dépend du résultat des clarifications.

Les cantons avec un IdM existant auront moins de travail à fournir que ceux qui n'en ont pas encore. Si le canton possède un IdM et présente les conditions pour une adhésion à la Fédération FIDES aucune ou alors seulement des adaptations dans le cadre du Life Cycle Management sont requises. Le projet de mise en œuvre sera plus conséquent si une IdM cantonale est disponible, mais doit être adaptée à la fédération FIDES ou qu'aucun IdM cantonal n'existe.

▪ Cantons sans IdM coordonnée par le canton

Les cantons qui n'ont pas d'IdM propre doivent d'abord engager des frais uniques pour le mettre en place. Un concept IdM cantonale fondée sur les concepts IT cantonales en place doit être définie. L'implémentation de l'IdM suppose ensuite l'exploitation de systèmes informatiques qui devront être mis à disposition ainsi que l'intégration d'applications IdM appropriées. Pour cela, le canton pourra se référer aux prescriptions de FIDES afin d'assurer la compatibilité de son infrastructure avec celle de la fédération. En ce qui concerne les compétences, l'introduction de l'IdM implique des tâches supplémentaires pour les personnes chargées d'assurer l'exploitation et l'entretien de l'infrastructure nécessaire. Les responsables au niveau de l'école sont les personnes les plus à même de se voir confier la saisie des identités. Mais suivant la manière dont l'IdM est conçu, cette mission peut également être déléguée à d'autres personnes.

▪ Cantons avec IdM coordonnée par le canton

En ce qui concerne les processus, les dépenses pour un IdM cantonal porteront sur la saisie des identités, l'exploitation et l'entretien des infrastructures informatiques nécessaires et, si cela n'a pas encore été fait, sur la création d'un IdM pour le canton. Au niveau de l'infrastructure, les systèmes informatiques cantonaux et leurs applications IdM requises pour ce dernier sont des charges déjà existantes. En ce qui concerne les compétences, des dépenses sont à inscrire au budget pour l'entretien des systèmes informatiques et des applications IdM. Des frais uniques seront engagés au niveau des bases normatives ainsi qu'éventuellement à celui de l'infrastructure si les clarifications effectuées avant la décision d'adhérer à la fédération ont montré que la stratégie IdM devait être adaptée.

3.3.4 Adhésion et participation

Dans la perspective de l'adhésion à la fédération, les cantons devront intégrer leurs IdP de l'IdM cantonal dans la fédération, ce qui peut entraîner un volume de travail très variable. Chaque canton devra également désigner une personne chargée de le représenter dans l'assemblée des participants. Enfin, des dépenses sont à prévoir pour les formations du personnel administratif et technique, pour les directions des écoles, pour les enseignants et pour les élèves. Toutes ces personnes doivent en effet être familiarisées avec les fonctions de la fédération.

3.4 Coûts de la Fédération FIDES

Dans les explications qui vont suivre et qui concernent le coût de la Fédération FIDES, nous ferons la distinction entre les coûts pour la mise en place de la Fédération et les coûts d'exploitation qui comprennent tous les coûts engendrés par la fourniture des prestations de la Fédération. Les montants indiqués sont des estimations, pour lesquelles les salaires sont évalués sur la base des Descriptions des fonctions-types de l'Ordonnance sur le personnel et des Tableaux des traitements du canton de Berne. Les montants calculés ont ensuite été comparés et validés avec ceux de la fédération des services d'identité qui existe déjà aux Pays-Bas (cf. Annexe II, *Bonnes pratiques de fédérations des services d'identités du domaine scolaire de pays européens*) et ceux du Service technique de SWITCHaai (cf. Annexe II, *Projets et bonnes pratiques de fédérations de services d'identités au plan national*).

Pour la mise en place Fédération, un total de CHF 1'840'000 doit être investi au cours des années 2018 et 2019. Les coûts d'exploitation s'élèvent à CHF 1'240'000 en 2019, et à partir de l'année 2020 des coûts d'exploitation annuels allant jusqu'à CHF 1'680'000 sont attendus.

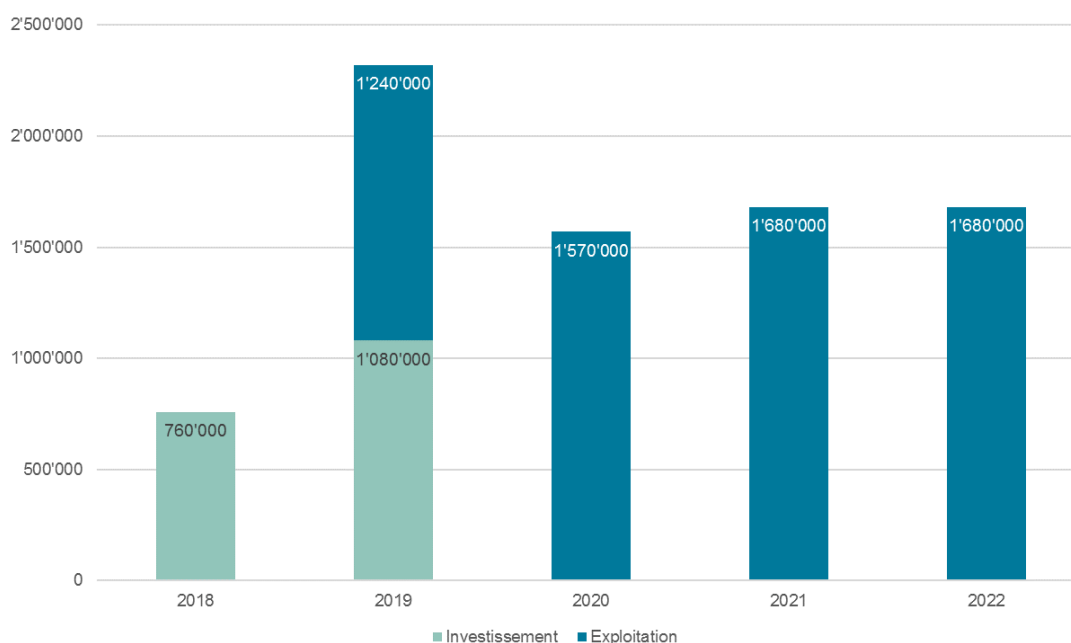


Figure 2 : Évaluation des coûts pour la mise en place et d'exploitation de la Fédération FIDES

3.4.1 Coûts d'investissement

Les dépenses d'investissement pour la mise en place de la Fédération FIDES comprennent tous les travaux nécessaires afin que l'organisation puisse être créée au début de l'année 2019. L'année 2018 sera essentiellement consacrée aux travaux préparatoires. La mise en place de l'équipe de gestion du Bureau de la Fédération, le recrutement et l'engagement du personnel et l'établissement des bases juridiques auront déjà commencé, tout comme la promotion de la Fédération FIDES auprès des parties prenantes concernées, en particulier la recherche des premiers participants.

Pour 2019, il est prévu d'intégrer dans la Fédération les IdP d'au moins dix cantons et les services d'au moins dix SP. Le travail de marketing pour le lancement de la Fédération doit donc être poursuivi. Une nouvelle charge de dépense en 2019 est la mise en place de l'infrastructure informatique et le conseil aux premiers cantons et SP participants. Des bases techniques seront documentées et mise à disposition pour les IdP et les SP qui adhèrent à la Fédération ultérieurement.

Coûts pour la mise en place	2018	2019
Mise en place de l'équipe de gestion du Bureau (y compris contrat de prestation, pilotage et gouvernance)	145 000	
Bases juridiques (y compris contrats, accords SLA/OLA, règlement)	290 000	
Recrutement et engagement (y compris recherche de personnel, évaluations et contrats de travail)	25 000	
Marketing (y compris promotion, documentation, site Internet et événements)	220 000	190 000
Mise en place de l'infrastructure informatique (y compris services techniques)		320 000
Conseils aux premiers participants (y compris intégration, pilotes, intégration technique)		460 000
Bases techniques pour les IdP et SP (y compris middleware, tests et directives)	80 000	110 000
Total des charges d'investissement	760 000	1 080 000

3.4.2 Coûts d'exploitation

La Fédération FIDES doit être créée pour le 1er janvier 2019 et c'est donc à partir de cette date qu'il y aura des charges d'exploitation. La première année, elles s'élèveront à Fr. 1 240 000. En 2020, elles atteindront Fr. 1 570 000 et en 2021 Fr. 1 680 000, augmentation imputable à l'adhésion de nouveaux cantons (et leurs IdP) et de nouveaux SP (et leurs services en ligne) à la Fédération. Ces évaluations reposent sur l'hypothèse qu'en 2020, le nombre des nouveaux SP excédera le nombre des nouveaux cantons adhérents. L'objectif est d'avoir en 2021 au moins dix-huit cantons et cent cinquante fournisseurs de services dont les IdP et les SP seront alors tous intégrés.

Coûts d'exploitation	2019	2020	2021	2021
Management (y compris direction, garantie de la qualité, management des processus et du risque, organes)	250 000	250 000	250 000	250 000
Administration (y compris administration, communication, comptabilité, rapports gestion du personnel)	200 000	200 000	200 000	200 000
Management du service (y compris marketing, démarchage, gestion des contrats, sorties)	190 000	190 000	190 000	190 000
Prestations de support (y compris hotline, documentation, formation)	130 000	240 000	360 000	360 000
Intégration technique (y compris IdP, SP, interfaces)		110 000	90 000	90 000
Entretien de l'infrastructure informatique (y compris administration système, entretien et exploitation, licences)	450 000	450 000	460 000	460 000
Services externes (sécurité, droit, technologie)	20 000	20 000	20 000	20 000
Innovation et développement		110 000	110 000	110 000
Total des charges d'exploitation	1 240 000	1 570 000	1 680 000	1 680 000

4 GLOSSAIRE

Terme	Définition du terme
Attributs standardisés	attributs d'une e-ID dont la structure et la signification sont convenus
Attributs pseudonymisés	attributs d'une e-ID qui ne permettent pas de remonter vers l'utilisateur ou utilisatrice final.
Authentification	processus d'examen d'une identité déclarée.
Autorisation	procédure de vérification du droit d'accès d'une entité authentifiée et de la délivrance de l'accès
Données personnelles	toutes les informations qui se rapportent à une personne identifiée ou identifiable (LPD, Art. 3)
Données d'utilisation (personnalisées)	données qui proviennent des utilisateurs finaux lors de l'utilisation d'un service en ligne. Elles sont traçables vers un utilisateur, une utilisatrice, on doit les comprendre comme étant personnalisées.
Données sur l'identité	données personnelles qui sont réunies dans une e-ID pour décrire une personne. Dans certains cas, l'on entend uniquement les informations destinées à assurer la connexion à un ordinateur ou à un service numérique.
e-ID (cantonale) pour la formation	e-ID pour la formation sous la responsabilité et organisée par un canton. Celle-ci peut consister en une solution centralisée ou fédérée au sein d'un canton. Elle permet d'accéder à des services en ligne utilisés dans l'ensemble du canton.
e-ID (nationale) pour la formation	e-ID pour la formation conforme au modèle de l'e-ID nationale pour la formation et qui est gérée par un canton qui participe à la Fédération des services d'identités pour l'espace suisse de formation. Il permet un accès, contrôlé par le canton, aux services en ligne de la Fédération.
e-ID (qui peut être fédérée au plan national) pour la formation	e-ID cantonale pour la formation conforme au modèle de l'e-ID nationale pour la formation.
e-ID pour la formation	e-ID utilisée pour l'accès aux services en ligne relevant d'une importance systémique dans le système éducatif suisse.
Espace numérique de formation	caractère numérique de l'espace de formation.
Fédération FIDES	nom de la Fédération des services d'identités pour l'espace suisse de formation, précédemment uniquement 'Fédération des services d'identités'.
Fournisseur d'identité (Identity Provider IdP)	composant technique qui stocke et fournit les identités numériques.
Fournisseur de services (Service Provider SP)	organisation qui exploite des services en ligne.
Gestion des identités (Identity Management IdM)	décrit l'administration des identités, la gestion des identités
Identification	procédure permettant de reconnaître sans équivoque une entité
Safety	fiabilité opérationnelle obtenue par des mesures techniques et organisationnelles.
Sécurité juridique (principe de)	principe de sécurité juridique assurant la prévisibilité et la cohérence de l'action gouvernementale. Il exige une réglementation des conditions juridiques claires, simples et prévisibles (protection contre une législation peu claire ou incomplète), pas de changements fréquents dans la législation, une jurisprudence aussi constante que possible et un système juridique stable fonctionnel.
Service en ligne	offre d'un prestataire de services

ANNEXE I : ASPECTS CENTRAUX DE LA FÉDÉRATION FIDES

1	Modèle de l'e-ID nationale pour la formation	19
1.1	Un minimum d'attributs nécessaires.....	19
1.2	Origine des données	19
1.3	Qualité des données	20
2	Principes, processus et standards de la Fédération FIDES.....	21
2.1	Principes de la Fédération FIDES	21
2.2	Processus de la Fédération FIDES	21
2.3	Technologies de la Fédération FIDES.....	21
3	Règlements et contrats.....	22
3.1	Règlements de la Fédération FIDES.....	22
3.2	Contrats de la Fédération FIDES	22
4	Scénarios pour la mise en place de la Fédération FIDES	23
4.1	Conditions pour la mise en route de l'exploitation de FIDES.....	23
4.2	Scénario A.....	23
4.3	Scénario B.....	24
4.4	Scénario C	25

1 MODÈLE DE L'E-ID NATIONALE POUR LA FORMATION

La construction, la structure et les valeurs admises des attributs de l'e-ID nationale pour la formation figurent dans le « Modèle de l'e-ID nationale pour la formation » qui constitue le standard de la Fédération FIDES. Le modèle se fonde sur les e-ID cantonales pour la formation. Il vise à rendre interopérables les attributs définis dans le cadre de la gestion cantonale des identités (IdM) ainsi que les valeurs qui ont été fixées pour chacun d'eux. En clair, les modèles cantonaux deviennent par ce moyen compatibles avec la Fédération. À noter que l'*identificateur universel et univoque* (UUID, abréviation d'Universally Unique Identifier) est le seul attribut qui est ajouté à l'e-ID cantonale pour la formation avec le modèle de l'e-ID nationale pour la formation. Il est généré et géré par le Service technique de la Fédération.

1.1 Un minimum d'attributs nécessaires

- **... pour la transmission de données de l'IdP au SP**
L'identificateur universel univoque est le seul attribut qui doit impérativement être communiqué pour l'authentification. Cet attribut permet de pseudonymiser l'utilisateur final et garantit en même temps qu'il peut être suffisamment reconnu.
- **... pour l'administration de l'e-ID pour la formation au sein de l'IdM**
L'utilisateur final doit pouvoir être corrélé de manière univoque avec son e-ID pour la formation. À cet effet, l'exploitant des IdM peut fixer et utiliser le numéro AVS, un numéro personnel ou toute autre référence qui permet une identification juridiquement suffisante de la personne physique. Pour gérer l'e-ID pour la formation, la Fédération FIDES requiert encore le nom d'utilisateur et le mot de passe personnel qui lui correspond.
- **... pour les SP**
Pour l'autorisation, les SP ont besoin d'autres données concernant les utilisateurs finaux. Des attributs importants sont par exemple :
 - le rôle (enseignant, élève, etc.)
 - l'établissement d'enseignement (nom de l'école)
 - le degré d'enseignement/l'année scolaire
 - la classe
 - le canton

Les SP pourraient requérir encore d'autres attributs de la Fédération. Il faut cependant noter ici que la combinaison de différents attributs non critiques rend possible l'identification sans équivoque d'une personne. Il apparaît donc que le nom d'une personne n'est pas suffisant pour une identification univoque. Mais si le nom est associé avec la date et le lieu de naissance ainsi qu'avec le domicile, données qui en soi ne sont pas critiques, un grand pas est franchi en direction d'une identification irréfutable.

1.2 Origine des données

L'identificateur universel univoque doit être généré, attribué et géré par un poste central afin que la transmissibilité de l'e-ID pour la formation puisse être garantie. Tous les autres attributs et valeurs sont définis par différentes sources — départements de l'instruction publique, services du personnel, administrations scolaires, directions scolaires, etc. — et transmis aux IdP.

1.3 Qualité des données

De manière générale, il faut viser à la meilleure qualité possible des données. Du fait de leurs origines décentralisées, ces données risquent d'être fournies de manière très hétérogène, raison pour laquelle cette exigence de qualité ne pourra être atteinte que moyennant un travail en amont considérable. L'effort pour assurer la qualité devra toutefois se maintenir dans un cadre raisonnable et doit donc bénéficier de l'aide des services de la Fédération FIDES. Le standard visé doit permettre que le soin et la qualité normalement apportés dans une école soient suffisants pour l'accès aux services en ligne via la Fédération.

2 PRINCIPES, PROCESSUS ET STANDARDS DE LA FÉDÉRATION FIDES

La création d'un espace de confiance tel que celui de la Fédération FIDES repose sur le fait de trouver un accord sur des principes, des processus et des standards communs et de s'y tenir. Toutes les parties concernées s'engagent par contrat à les respecter et à les appliquer pour tout ce qui concerne l'e-ID pour la formation.

Les normes eCH, définies dans le cadre de l'initiative de la Stratégie suisse de cyberadministration, servent de base pour le concept de la Fédération. En particulier, sont considérées les standards eCH qui concernent l'identité numérique.

2.1 Principes de la Fédération FIDES

L'identification des utilisateurs finaux se fait avec la plus grande fiabilité possible (cf. Annexe I, *Modèle de l'e-ID nationale pour la formation*). A cet effet, les données des e-ID cantonales pour la formation doivent être activement gérées et très régulièrement tenues à jour.

Les données personnelles des utilisateurs finaux associées à l'e-ID pour la formation sont protégées de tout accès non autorisé ou abus de la part des partenaires associés à la Fédération FIDES avec les moyens informatiques les plus modernes.

Les données générées par l'utilisation des services en ligne ne sont pas transmises à des tiers ni exploitées en vue d'une utilisation commerciale. Conformément à leurs obligations contractuelles, les SP déclarent de manière explicite comment les données générées lors de l'utilisation de leurs services en ligne sont ensuite traitées et utilisées. Dans tous les cas, le principe de l'option d'adhésion s'applique pour l'exploitation ultérieure de données des utilisateurs. En clair, cela signifie que les utilisateurs finaux doivent être priés de donner leur consentement explicite avant de se voir proposer d'autres offres du SP.

2.2 Processus de la Fédération FIDES

Des processus contraignants garantissent un niveau élevé de fiabilité. Les activités sortant du cadre de l'organisation mais restant dans le contexte de la Fédération FIDES sont documentées et transparentes pour tous les participants.

Toutes les informations concernant la Fédération sont rapidement rendues accessibles à tous les participants.

Les plans d'urgence affectant encore d'autres organisations permettent une intervention rapide et fiable en cas d'incident mettant en danger la sécurité au sein de la Fédération. Les responsables et les interlocuteurs sont connus de tous les participants.

Les participants sont activement intégrés et de manière compréhensible à tout processus de développement de la Fédération.

2.3 Technologies de la Fédération FIDES

Les participants à la Fédération FIDES utilisent le standard OASIS SAML2 pour l'annonce sécurisée des utilisateurs finaux ainsi que pour le transfert protégé des attributs de l'e-ID pour la formation. Ce standard est utilisé aussi bien par un grand nombre de produits commerciaux que par des logiciels à code ouvert et libre. D'autres développements prévoient OpenID Connect ou OAuth2. Ces standards ne présentent toutefois pas encore la stabilité suffisante pour une fédération de services d'identité.

L'authentification des composants techniques entre eux fait intervenir des certificats numériques selon UIT-T Standard X509v3.

Par ailleurs, la Fédération utilise le protocole HTTPS pour l'échange de données et d'informations cryptées. Les transferts de données et les services web recourent à l'architecture REST pour le codage des données.

3 RÈGLEMENTS ET CONTRATS

La cohésion de la Fédération FIDES perçue comme un ensemble est assurée par des règlements et des contrats. Ces documents seront élaborés pendant la phase de mise en place de la Fédération. Les cantons qui auront adhéré à la Fédération à ce moment seront consultés pour ces travaux.

3.1 Règlements de la Fédération FIDES

Les règlements de la Fédération FIDES sont des documents normatifs visant à assurer une exploitation sans heurts de celle-ci. Ils font partie des contrats, sont émis sous la houlette du Bureau de la Fédération et sont contraignants pour les participants à la Fédération.

- **Statuts de la Fédération**
Les statuts de la Fédération décrivent la structure de son organisation et définissent les rôles, les fonctions, les droits et les devoirs de chaque acteur de la Fédération. Ils définissent notamment comment le Bureau se constitue, comment l'assemblée des participants se déroule et comment ces deux entités interagissent.
- **Règlement de service et accords sur le niveau de service**
Le Règlement de service consigne de façon détaillée et décrit toutes les offres de la Fédération et ses services. Certains accords sur le niveau de service (SLA) assureront aux parties contractantes les services de la Fédération.

3.2 Contrats de la Fédération FIDES

Convention de prestations

La convention sur les prestations règle les relations entre les mandants et l'organisation mandataire. Elle contient le mandat pour la mise en place et l'exploitation de la Fédération FIDES sur la base du concept-cadre de la Fédération. Le ou la mandataire propose la Fédération comme un service et assume la responsabilité du Bureau. Le financement est défini dans la convention de prestations.

Contrat de prestations

Un contrat de prestations devra être signé entre le Bureau de la Fédération et l'organisation qui exploitera le Service technique si celui-ci n'est pas exploité par la même organisation que le Bureau.

Contrat de participation

Les contrats de participation règlent les droits et les obligations des participants et sont signés par le Bureau de la Fédération et le canton participant (Département de l'instruction publique) ou entre le Bureau et les SP participants. Le contrat de participation précise aussi les critères d'admission des SP dans la Fédération.

4 SCÉNARIOS POUR LA MISE EN PLACE DE LA FÉDÉRATION FIDES

Les scénarios ci-dessous pour la mise en place de la Fédération FIDES se réfèrent aux activités menées entre la décision de l'assemblée plénière de la CDIP et le début de l'exploitation de la Fédération. Tous trois visent à préparer les conditions nécessaires pour mettre en œuvre l'exploitation de la Fédération. Les variables de ces scénarios sont les suivantes :

- le nombre de participants à l'ouverture de l'exploitation
- la disposition dans le temps de la décision d'adhésion d'autres participants, durant le cours de l'exploitation.

4.1 Conditions pour la mise en route de l'exploitation de FIDES

Les conditions préalables suivantes doivent être créées ou discutées pour le début de l'exploitation de la Fédération FIDES dans le cadre de la première phase de mise en place :

- décisions portant sur les organisations qui seront chargées du Bureau et du Service technique
- détermination des standards de la Fédération concernant la technique, les processus et l'organisation
- conclusion de contrats de participation par un nombre minimum de cantons
- conclusion de contrats de participation par un nombre minimum de SP
- les cantons participants ont mis en place un IdM pour au moins un domaine partiel de leur système scolaire et ont implémenté les standards de la Fédération
- les SP participants ont implémenté les standards de la Fédération
- les services centraux pour l'organisation et la technique sont prêts

4.2 Scénario A

Hypothèse :

- Un nombre minimum de cantons confirme sa participation
- Aucune participation connue de SP

Scénario :

La CDIP désigne l'organisation avec laquelle elle convient d'une convention de prestation pour le Bureau de la Fédération FIDES. Le Bureau se constitue et décide de l'organisation du Service technique. Le Bureau établit la liste des cantons participants lors de l'entrée en fonction de la Fédération. Le Bureau élabore les documents contractuels nécessaires pour la participation et conclut des contrats avec les cantons participants. Le Bureau décide avec les cantons participants les SP qui doivent être admis au sein de la Fédération dès le début de l'exploitation. Le Bureau et les cantons participants conviennent de critères pour l'admission de nouveaux SP. D'entente avec les cantons, le Bureau élabore les exigences de protection des données pour les SP. Les cantons participants qui n'ont pas de gestion des identités IdM en réalisent une avec l'aide du Bureau. Le Bureau acquiert, fait développer ou développe en régie propre les logiciels nécessaires pour les services centraux. Le Bureau crée une plate-forme d'essai pour les IdP et les SP afin que ceux-ci puissent vérifier que les différents systèmes techniques fonctionnent ensemble. Les cantons participants possédant leurs propres gestions des identités IdM élaborent les interfaces nécessaires avec l'aide du Service technique de la Fédération. Le Bureau négocie avec les SP souhaités leur adhésion à la Fédération et élabore ou conclut avec eux les contrats nécessaires. D'entente avec les participants, le Bureau définit le modèle de l'e-ID afin de fixer la structure et le contenu des e-ID pour la formation. De même, il fixe les processus pour les activités qui ne concernent pas uniquement l'organisation. Avec l'aide du Service technique, les SP adaptent leurs systèmes aux standards techniques de la Fédération. Le Bureau commence l'exploitation de la Fédération avec les cantons participants et les SP (cf. [chapitre 3.1](#)).

Avantages	Inconvénients
+ Pas de mobilisation de personnel supplémentaire pour l'enregistrement des IdP et des SP + Possibilité de collaboration étroite avec les cantons si le nombre de participants est petit au début avec à la clé une meilleure identification des besoins + La prise en compte des participants permet une exploitation stable et satisfaisante	- Frais de marketing élevés pour l'acquisition de SP - Un nombre peu élevé de SP au début de l'exploitation de la Fédération pourrait réduire l'utilité de celle-ci - Travaux de détail importants qui ralentissent la mise en route de la Fédération FIDES

4.3 Scénario B

Hypothèse :

- Un nombre minimum de cantons confirme sa participation
- On sait qu'il y aura un petit nombre de SP participants

Scénario :

La CDIP signe avec le Bureau de la Fédération FIDES une convention de prestations. Le Bureau se constitue et décide de l'organisation du Service technique. Le Bureau élabore les documents contractuels nécessaires pour la participation et conclut des contrats avec les cantons participants. Les cantons participants qui n'ont pas leur propre gestion des identités IdM la mettent en place avec l'assistance du Bureau. Le Bureau acquiert, fait développer ou développe en régie propre les logiciels nécessaires pour les services centraux. Le Bureau crée une plate-forme d'essai pour les IdP et les SP afin que ceux-ci puissent vérifier que les différents systèmes techniques fonctionnent ensemble. Les cantons participants possédant leurs propres gestions des identités IdM élaborent les interfaces nécessaires avec l'aide du Service technique de la Fédération. Le Bureau négocie avec les SP connus leur adhésion à la Fédération et élabore ou conclut avec eux les contrats nécessaires. Avec l'aide du Service technique, les SP adaptent leurs systèmes aux standards techniques de la Fédération. Le Bureau commence l'exploitation de la Fédération avec les cantons participants et les SP.

Avantages	Inconvénients
+ Pas de mobilisation de personnel supplémentaire pour l'enregistrement des IdP et des SP + Possibilité de collaboration étroite avec les cantons si le nombre de participants est petit au début avec à la clé une meilleure identification des besoins	- Un nombre peu élevé de SP au début de l'exploitation de la Fédération pourrait réduire l'utilité de celle-ci

4.4 Scénario C

Hypothèse :

- Tous les cantons confirment leur participation
- On sait qu'il y aura un grand nombre de SP participants

Scénario :

La CDIP signe avec le Bureau de la Fédération FIDES une convention de prestations. Le Bureau se constitue et décide de l'organisation du Service technique. Le Bureau conclut des contrats avec les cantons participants. Les cantons participants qui n'ont pas leur propre gestion des identités IdM la mettent en place avec l'assistance du Bureau. Le Bureau acquiert, fait développer ou développe en régie propre les logiciels nécessaires pour les services centraux. Le Bureau crée une plate-forme d'essai pour les IdP et les SP afin que ceux-ci puissent vérifier que les différents systèmes techniques fonctionnent ensemble. Les cantons participants possédant leurs propres gestions des identités IdM élaborent les interfaces nécessaires avec l'aide du Service technique de la Fédération. Le Bureau négocie avec les SP connus leur adhésion à la Fédération et élabore ou conclut avec eux les contrats nécessaires. Avec l'aide du Service technique, les SP adaptent leurs systèmes aux standards techniques de la Fédération. Le Bureau commence l'exploitation de la Fédération avec les cantons participants et les SP.

Avantages	Inconvénients
+ Grande offre de services en ligne dès l'ouverture de l'exploitation	- Charges de personnel élevées durant la phase de mise en place - Forte complexité jusqu'à l'ouverture de l'exploitation

ANNEXE II: CONTEXTE DE LA FÉDÉRATION FIDES

1	Ecosystème e-ID pour la formation.....	27
1.1	Projet avec la Haute école spécialisée bernoise	27
1.2	Situation initiale hétérogène – fragmentation persistante	27
1.3	Défis, facteurs de succès critiques	27
1.4	Scénario sans Fédération	28
2	Bonnes pratiques concernant les solutions cantonales d'e-ID pour la formation.....	29
2.1	Canton de Berne	29
2.2	Canton de Bâle-Campagne	30
2.3	Canton du Valais	30
2.4	Canton de Neuchâtel.....	31
2.5	Canton du Jura.....	31
3	Projets et bonnes pratiques de fédérations de services d'identités au plan national	33
3.1	SWITCHaai	33
3.2	SWITCH edu-ID	34
3.3	SuisseID.....	35
3.4	Swisscom Mobile ID	35
3.5	Fédération suisse d'identités (FSI).....	36
3.6	Office fédéral de la police fedpol	36
4	Bonnes pratiques de fédérations des services d'identités du domaine scolaire de pays européens	37
4.1	Danemark : UNI-Login.....	37
4.2	Estonie : HarID	37
4.3	Pays Bas : Entree Federatie	38
4.4	Suède : Skolfederation	38

1 ECOSYSTÈME E-ID POUR LA FORMATION

Ayant pour ambition de fédérer les services d'identités de l'espace suisse de formation, le projet FIDES se situe dans un contexte complexe caractérisé par l'interaction de conditions, acteurs, fonctions et utilisations des identités numériques. La connaissance de ces interactions, ainsi que des éléments qui les sous-tendent, sont essentiels pour les réflexions conceptionnelles du projet FIDES, pour guider les parties prenantes ainsi que pour le succès de la mise en œuvre de la Fédération.

1.1 Projet avec la Haute école spécialisée bernoise

Sur mandat de educa.ch, le centre Digital Society de la Haute école spécialisée bernoise (BFH) a réalisé un modèle d'écosystème e-ID pour la formation (ISCED 020-4). Il s'est fondé pour cela sur ses travaux réalisés pour le SECO portant sur une e-ID pour la formation couvrant l'ensemble de la Suisse³. Le modèle montre des liens et des dépendances de l'interaction de solutions IAM dans le contexte de la formation et contribue à une utilisation uniforme de la terminologie et à une intelligibilité générale du sujet. À l'aide de ce modèle qui devait servir de base de discussion, des analyses détaillées ont été menées sous forme d'interviews et d'ateliers sur l'utilisation actuelle d'identités numériques dans le système éducatif suisse. De plus, les avis des différents acteurs par rapport à la situation visée en vue d'une solution de Fédération, ont été demandés⁴. Les bases ont ainsi pu être élaborées pour décider des mesures à prendre sur un plan général qui sont propres à assurer le succès durable de l'utilisation d'e-ID pour la formation.

1.2 Situation initiale hétérogène – fragmentation persistante

Il apparaît dans le système éducatif suisse que les solutions IAM et e-ID sont très hétérogènes et peuvent fortement varier en fonction du canton, du contexte (enseignement et administration) et/ou du degré scolaire. On peut pratiquement admettre que toutes les écoles ou les communes scolaires ainsi que les administrations cantonales de l'instruction publique utilisent aujourd'hui une ou plusieurs solutions d'identification électronique. C'est en premier lieu le cas pour les enseignants et le personnel de l'administration de la formation mais aussi de plus en plus pour l'utilisation par les élèves. Suivant les acteurs et les éléments de l'écosystème impliqués dans les différentes solutions (par exemple sources de données privées ou, à l'opposée, registres de droit public), ces solutions varient fortement quant à la qualité des données d'identité, la protection des données et la sécurité juridique.

1.3 Défis, facteurs de succès critiques

Le modèle de l'écosystème e-ID pour la formation met en évidence l'importance d'une interaction ordonnée entre les différents acteurs (cantons, IdP, SP) pour des solutions e-ID et IAM efficaces, sûres et conformes aux exigences de la protection des données. Cela requiert une collaboration active entre les différentes parties qui ont chacune des besoins propres (plus l'exigence de pilotage au niveau cantonal est élevée, plus les SP réagiront par exemple de manière critique). Ce seront donc surtout les différences cantonales dans l'organisation de l'enseignement (y compris les différences spécifiques aux degrés scolaires) qui constitueront un défi particulier. Outre l'exigence générale de fiabilité, les critères de flexibilité et de rapidité devront toujours être pris en compte. Comme la valeur ajoutée naît en particulier de la disponibilité et de l'accessibilité des services externes et des prestataires de contenus, les cantons veulent avoir une garantie que les SP qui leur sont importants participeront

³ Berner Fachhochschule (Hg.) (2015). *eID-Ökosystem Modell. Projektabschlussbericht*. https://www.wirtschaft.bfh.ch/uplo-ads/tx_frppublikationen/eID-OEkosystem_V1_2.pdf

⁴ Les rapports des différents chapitres du projet de la Haute école spécialisée bernoise seront disponibles à partir de l'été 2017 sur la plate-forme d'information educa.ch.

à la Fédération. À l'inverse, la valeur ajoutée pour les SP n'existe que si tous les cantons, dans la mesure du possible, adhèrent à la Fédération.

1.4 Scénario sans Fédération

Pour conclure, un scénario sans Fédération montre la perspective d'avenir dans laquelle le système éducatif mis au défi par la numérisation doit s'en sortir sans solution de fédération. Il en ressort clairement que sans l'établissement d'une Fédération de services d'identités pour la formation à l'échelon national, la fragmentation du paysage e-ID empêchera une collaboration efficiente, sûre et conforme aux exigences de la protection des données entre les enseignants, les élèves, les administrations scolaires et d'autres acteurs. Les solutions de remplacement à la Fédération ne sont pas en mesure de convaincre. On pourrait par exemple imaginer la création d'identités pour le secteur de la formation inspirée d'une solution e-ID nationale (cf. Annexe II, *Projets et bonnes pratiques de fédérations de services d'identités au plan national*). Mais comme une telle solution n'est pas en mesure de fournir les preuves de fonctions et d'autres attributs spécifiques au système éducatif, une fédération nationale reste nécessaire pour les attributs supplémentaires. Le caractère facultatif de l'obtention d'une telle e-ID, sans garantie d'utilisation pour l'ensemble du territoire suisse, constitue un défi supplémentaire.

2 BONNES PRATIQUES CONCERNANT LES SOLUTIONS CANTONALES D'E-ID POUR LA FORMATION

Entre février et mars 2017, l'équipe de projet FIDES a rencontré les personnes de référence cantonales des cantons de Berne, Bâle-Campagne, Valais, Neuchâtel et Jura. Le but était de recueillir des informations récentes concernant les solutions cantonales IdM dans ces cantons. Les informations collectées donnent un aperçu de la situation cantonale dans le domaine de l'identité numérique, les solutions mises en œuvre et l'état de préparation pour une entrée du canton dans la Fédération FIDES.

2.1 Canton de Berne

2.1.1 Situation

Il n'existe pas de base légale qui, au niveau cantonal, puisse légitimer la mise en place d'un IdM centralisé pour les écoles des degrés obligatoires et non obligatoires. Toutefois, la plupart d'entre elles, en particulier les grandes institutions du degré secondaire II relevant de la compétence cantonale ont leur propre IdM.

Au degré primaire, l'IdM est de la responsabilité des communes et n'est que partiellement centralisé puisque plusieurs écoles ont leurs propres IdM. L'IdM au niveau communal est donc très hétérogène et peu standardisé.

2.1.2 Solution utilisée

Le département informatique de la Direction de l'instruction publique du canton de Berne propose un ensemble de produits appelé « EDUBERN » avec des services et des logiciels adaptés aux écoles et que ces dernières peuvent utiliser moyennant finance. Ce portefeuille se base en grande partie sur des technologies développées par Microsoft. Quelques institutions, parmi lesquelles quatre gymnases et six écoles professionnelles utilisent notamment l'offre « Cloudomat » qui comprend plusieurs services ainsi que la mise à disposition d'une e-ID cantonale pour la formation. De ce fait, l'Office des services centralisés de la Direction de l'instruction publique exerce le rôle d'un IdP sur mandat de ces écoles et exploite l'IdM dans le cadre de l'infrastructure des technologies de l'information de la DIP.

Les données servant à l'établissement d'e-ID pour les utilisateurs du degré secondaire II proviennent principalement de la solution pour administration d'école « Evento ». Celle-ci est exploitée de façon centralisée par l'Office de l'enseignement secondaire du 2e degré et de la formation professionnelle du canton de Berne. Elle gère des données concernant des informations (attributs) de cadres des écoles et d'enseignants (environ 5000 personnes) ainsi que des données des élèves (environ 60 000).

L'Office des services centralisés de la direction de l'instruction publique se positionne comme un centre de compétences pour les services de technologies de l'information destinés au système éducatif cantonal. Un projet pilote du portefeuille « EDUBERN » propose également des services aux écoles du degré primaire.

2.1.3 Disponibilité pour la Fédération FIDES

Les bases pour une adhésion à la Fédération des services d'identité existent. Les solutions réalisées au degré secondaire conviennent pour une adhésion. Il reste à mettre en place une coordination cantonale des solutions décentralisées. La marche à suivre pour une solution destinée au degré secondaire I et à l'école primaire doit encore être discutée.

2.2 Canton de Bâle-Campagne

2.2.1 Situation

Depuis que la solution d'administration des écoles SAL a été entièrement introduite, en août 2016, quatorze écoles primaires ainsi que les écoles secondaires et les gymnases sont raccordés au même système informatique. Le fait que trois niveaux de scolarité reposent sur la même solution IT et que l'on ait un même IdM centralisé pour les élèves, les enseignants, les directions d'école, les secrétariats d'école et d'autres membres du personnel scolaire constitue en soi une particularité notable. La condition préalable pour l'exploitation de cet IdM réside dans des bases juridiques qui ont été approuvées par le législatif cantonal. Les écoles professionnelles cantonales sont également intégrées dans l'IdM centralisé mais avec une autre solution d'administration. En outre, des écoles primaires administrées par les communes possèdent en partie un autre IdM séparé. Enfin, la bibliothèque cantonale exploite son propre IdM.

2.2.2 Solution utilisée

Les informations nécessaires pour établir les e-ID nécessaires proviennent en général de la solution d'administration scolaire SAL. Le répertoire exploité dans l'infrastructure cantonale comprend actuellement environ 17 000 e-ID dont environ 4500 sont des utilisateurs identifiés du degré secondaire II. Ce sont aujourd'hui principalement les deux services SAL et Microsoft Office 365 Education qui sont utilisés. Par ailleurs, un accès permettant d'obtenir des services tels que par exemple nanoo.tv (diffusion de films et émissions télévisées), le projet Neptun (acquisition de matériel informatique) et la gestion de logiciels sur des appareils mobiles doit être testé. L'accès aux ressources numériques, en particulier des éditions scolaires cantonales, constitue un autre scénario essentiel qui devrait être utilisé à l'avenir.

2.2.3 Disponibilité pour la Fédération FIDES

Avec son IdM géré de façon centralisée et couvrant les trois niveaux de scolarité, le canton de Bâle-Campagne a mis en place une solution qui demeure remarquable. D'un point de vue organisationnel et technique, les conditions pour une adhésion à la Fédération FIDES sont remplies.

2.3 Canton du Valais

2.3.1 Situation

Le canton du Valais offre différents services en ligne pour ses établissements scolaires (Moodle, Educanet², Microsoft Office 365, plateforme multimédias, gestion administrative, ...). Ces services numériques sont supervisés par le centre de compétences ICT-VS, rattaché au Département de l'économie et de la formation (DEF). Les écoles cantonales (secondaire II) disposent d'une infrastructure centralisée avec un accès unifié à la plupart des services proposés. Pour les écoles de la scolarité obligatoire (primaire, secondaire I), il appartient aux communes de prendre en charge l'infrastructure d'accès aux services numériques.

2.3.2 Solution utilisée

Pour faire évoluer l'accès au système d'information scolaire cantonal (et intercantonal), le centre ICT-VS vise à déployer une solution de gestion des identités et des accès centralisée (IAM). Il s'agit d'attribuer un « login cantonal unique » à tous les enseignants, les élèves, voir à terme aux parents afin de leur permettre d'accéder en ligne à l'ensemble des services auxquels ils ont droit (SSO).

La création des identités numériques se fonde sur deux référentiels de données cantonaux (Escada, ISM) contenant tous les attributs scolaires pour les niveaux : primaire, secondaire I et secondaire II (professionnels et écoles du degré secondaire supérieur). A terme, le registre des habitants sera également un référentiel.

La solution « IAM pédagogique » au niveau cantonal est en phase de test. Le but affirmé du Département de la formation est d'offrir aux écoles du canton un véritable « environnement numérique de travail » pour la rentrée scolaire 2018.

2.3.3 Disponibilité pour la Fédération FIDES

Le projet IAM du Valais a pris en compte la Fédération FIDES dès sa conception. Les technologies utilisées (SAML notamment) sont compatibles. Le modèle d'identité numérique et les standards utilisés pourront s'adapter à ceux de la Fédération. À ce stade, il n'y a pas d'obstacle au point de vue tant technique qu'organisationnel. Lorsque le Département de la formation aura mis en service son « IAM pédagogique », le canton du Valais sera techniquement prêt à entrer dans la Fédération.

2.4 Canton de Neuchâtel

2.4.1 Situation

La base d'un projet cantonal IdM dans le canton de Neuchâtel repose sur plusieurs acquis comme le Réseau pédagogique neuchâtelois (RPN), mis en service en juin 1999, auquel les écoles du canton de Neuchâtel sont reliées. Celui-ci est la colonne vertébrale en termes de télécommunication pour toutes les écoles neuchâteloises obligatoires et post obligatoires. Un autre acquis est le projet cantonal ICT 01-04 visant un équipement progressif de toutes les écoles depuis 2001 et mettant en œuvre une politique publique en faveur de l'intégration des médias, images, technologies de l'information et de la communication (MITIC) dans les écoles neuchâteloises. Celle-ci est ciblée sur les infrastructures techniques, la formation des utilisateurs et l'harmonisation de certains processus administratifs. Un troisième acquis est le déploiement du système d'information CLOEE gérant les données principales des élèves et des enseignants du canton (scolarité obligatoire, post obligatoire (formation gymnasiale et professionnelle) et la scolarité spécialisée).

2.4.2 Solution utilisée

Avec CLOEE, le canton dispose déjà d'une solution pour la gestion des identités du RPN, à partir d'un système de centralisation des données personnelles. Les login RPN peuvent déjà être utilisés, par exemple, pour se connecter sur la plateforme du plan d'études romand.

2.4.3 Disponibilité pour la Fédération FIDES

En l'état, il n'y a pas d'obstacles à l'entrée du canton de Neuchâtel dans une future fédération des services d'identités. Sitôt la décision d'adhésion prise par le Département de l'éducation et de la famille (DEF), la connexion à la Fédération FIDES d'un IdM cantonal, basé sur le RPN et des données stockées dans la base de données CLOEE, serait du ressort de l'office de l'informatique scolaire et de l'organisation, entité responsable du RPN pour les écoles obligatoires.

2.5 Canton du Jura

2.5.1 Situation

Dans le canton du Jura, la question d'une solution centralisée SSO pour accéder à des services en ligne est pour l'instant en suspens. Le projet cantonal pour une solution centralisée IdM reposera sur une exportation anonymisée de la base de données CLOEE (conjointe au canton de Neuchâtel et du Jura). Le principe doit encore obtenir l'aval du Département de l'Éducation. La situation actuelle est que les chefs d'établissements souscrivent directement des contrats avec les SP, en partie sans coordination cantonale.

2.5.2 Solution utilisée

Il sera possible de créer des identités numériques sur base des données contenues dans la base CLOEE. La base de données sécurisée CLOEE contient toutes les données scolaires des niveaux primaires et secondaires pour les enseignants et les élèves (dossier de l'élève). Exportée quotidiennement elle permettra la création et l'entretien des identités numériques pour l'accès à des services en ligne.

2.5.3 Disponibilité pour la Fédération FIDES

Le canton du Jura ne pourra participer à la Fédération FIDES que lorsque le projet cantonal IdM aura reçu l'aval des autorités cantonales.

3 PROJETS ET BONNES PRATIQUES DE FÉDÉRATIONS DE SERVICES D'IDENTITÉS AU PLAN NATIONAL

A côté du projet de Fédération FIDES, d'autres exemples et initiatives dans le domaine de l'identité numérique existent en Suisse. Ces exemples ont nourri la réflexion conceptuelle du projet FIDES ainsi que les choix technologiques entrepris. Un exemple a particulièrement eu une influence sur le projet, la fédération des services d'identités mise en place dans le niveau tertiaire SWITCHaai. D'autres exemples d'utilisation d'identité numérique fédérées ou de services single sign-on existants, ou en projet, sont mentionnés ci-dessous. Il est important de suivre l'évolution d'autres projets et initiatives et de s'assurer de la compatibilité des systèmes et des technologies employées par la Fédération. Ceci permettra, à terme, de pouvoir perfectionner la Fédération. La compatibilité des systèmes permettra d'utiliser des identifiants externes pour s'authentifier sur des services en ligne de la Fédération.

3.1 SWITCHaai

3.1.1 Une fédération des services d'identités.

SWITCHaai Federation est une fédération des services d'identités pour le secteur de l'enseignement supérieur et de la recherche en Suisse et au Liechtenstein. L'idée initiale était de créer une infrastructure permettant de mutualiser l'accès aux services web pour les institutions du degré tertiaire. La Fédération SWITCHaai est une expérience réussie de plus de dix ans dans le domaine.

3.1.2 Participants

Les participants à la fédération sont les « membres de la fédération » et les « partenaires de la fédération ». Les membres de la fédération font partie de la communauté SWITCH en tant que « home organisation » et sont fournisseurs d'un service d'identités numériques pour leurs utilisateurs (IdP), ils peuvent aussi disposer de services en ligne (SP). Seules les organisations de l'enseignement supérieur ou de recherche en Suisse et au Liechtenstein peuvent devenir membres de la fédération.

Les organisations suivantes sont membres de la communauté SWITCH : universités cantonales, Ecoles polytechniques, instituts de recherche des EPF, hautes écoles pédagogiques, hautes écoles spécialisées et l'Institut fédéral des hautes études en formation professionnelle (IFFP).

Les partenaires de la fédération offrent un ou plusieurs services en ligne (SP comme des plateformes e-Learning, Email...) à au moins un membre de la fédération (système de parrainage). Cependant les partenaires de la fédération ne sont généralement pas autorisés à fournir un service d'identité numérique (IdP) dans la fédération. Les partenaires peuvent aussi être des organisations situées en dehors de la Suisse.

3.1.3 Services

Le service de base de la fédération est SWITCHaai, l'infrastructure d'authentification et d'autorisation mise en place par SWITCH. L'architecture technique comporte un annuaire de métadonnées central décrivant les membres de la fédération et les partenaires de la fédération.

Les universités enregistrent et créent, elles-mêmes, les identités numériques pour les étudiants, enseignants et employés lors de leur inscription ou recrutement dans l'établissement de troisième cycle. Avec un login unique, les utilisateurs finaux peuvent accéder à des services comme une solution e-Learning ou des accès Wi-Fi de plusieurs universités.

Il y a plus de 1000 services attachés à la fédération.

3.1.4 Architecture technique

L'architecture technique de SWITCHaai utilise la technologie open source Shibboleth pour la gestion des identités numériques au sein d'une fédération et est basée sur le standard open source SAML (Security Assertion Markup Language).

Le choix de la technologie de SWITCHaai est compatible avec la Fédération FIDES qui utilise ces mêmes technologies et standards. La compatibilité entre la Fédération et SWITCHaai et son successeur SWITCH edu-ID est importante car elle permettra d'établir des passerelles entre les degrés secondaire II et tertiaire pour une identité numérique qui « suit » l'utilisateur pendant toute sa scolarité pour un apprentissage tout au long de la vie.

L'architecture technique de la fédération SWITCHaai et de la Fédération FIDES permettent de rejoindre d'autres fédérations basées sur le modèle AAI, par exemple à travers la connexion à eduGAIN, une fédération de fédérations interconnectées à l'échelle planétaire dans le domaine de l'éducation et de la recherche.

3.1.5 Gestion de la fédération

SWITCH est chargé de la gestion de l'infrastructure technique centrale de la fédération et de maintenir le cercle de confiance établi entre les membres et les partenaires de la fédération. Ceux-ci doivent signer un contrat de services (services agreement) avant de joindre la fédération. Le contrat, passé entre SWITCH et les membres ou les partenaires les oblige légalement à accepter certaines responsabilités et respecter la politique de confidentialité des données.

La coordination de SWITCHaai est soutenue par deux comités. SWITCH consulte le comité consultatif AAI (AAI Advisory Committee) et le groupe communautaire AAI (AAI Community Group) pour obtenir des conseils et avis sur le développement à long terme et l'optimisation administrative et technique de la fédération. Le comité consultatif AAI est composé des représentants des membres de la fédération (IdP) ainsi que des représentants de différents groupes de services, et de SWITCH. Le groupe communautaire SWITCH est composé de tous les représentants des organisations de la communauté SWITCH qui sont participants à la fédération.

3.1.6 Financement

Les membres de la fédération contribuent dans le cadre de leur engagement envers SWITCH, qui se charge de l'opération de la fédération.

3.2 SWITCH edu-ID

3.2.1 Une fédération d'identités

SWITCH edu-ID est la continuation de SWITCHaai et remplacera celle-ci dans un futur proche. A la différence de SWITCHaai qui fédère des services d'identités, SWITCH edu-ID est un projet de fédération d'identités numériques, avec un fournisseur d'identités numériques unique (IdP). Le projet de migration vers le service SWITCH edu-ID s'achèvera en 2020 quand toutes les organisations auront migré de SWITCHaai vers SWITCH edu-ID. Pour se faire, elles doivent de façon individuelle définir un projet de migration et le mettre en œuvre en coopération avec SWITCH.

Dans ce modèle, les attributs décrivant leur rôle dans l'organisation sont, comme avec SWITCHaai, gérés par les universités. Cependant, à la différence de SWITCHaai, avec SWITCH edu-ID les utilisateurs eux-mêmes doivent créer leurs identités.

3.2.2 Transfert des utilisateurs

Le fournisseur d'identité central sera mis à disposition pour les anciens utilisateurs de SWITCHaai, mais aussi pour tout autre utilisateur qui souhaite utiliser le service SWITCH edu-ID. Tous les utilisateurs de SWITCHaai sont, à terme, invités à être transférés dans le nouveau système IdM SWITCH edu-ID.

3.2.3 Services

Par contre, au niveau des services, aucune modification ne sera nécessaire. Pourtant, la SWITCH edu-ID apportera des fonctionnalités additionnelles dont les services pourraient profiter. Cela nécessitera certaines adaptations.

3.2.4 Gestion de la fédération

La mise en place de la SWITCH edu-ID se déroule directement dans la fédération SWITCHaai.

3.2.5 Financement

Le financement de la SWITCH edu-ID suit le modèle financier de SWITCHaai.

3.3 SuisseID

3.3.1 Signatures numériques

La SuisseID est née à la suite de la loi fédérale sur la signature électronique (2003), révisée en 2016 et entrée en vigueur le 1er janvier 2017. Celle-ci introduit un nouvel alinéa dans le code des obligations (art. 14 al. 2bis CO) qui prévoit que tous les contrats soumis à la forme écrite pourront être également conclus par la voie électronique.

SuisseID a été officiellement lancée en 2010 par la Confédération et mise en œuvre par le Secrétariat d'État à l'économie (SECO) pour promouvoir les transactions électroniques et soutenir l'économie suisse en général, particulièrement l'économie numérique. Elle permet de réaliser une signature électronique reconnue sur le plan juridique pour des documents officiels tels que des contrats.

Le service est fourni par des prestataires reconnus conformément à la loi sur la signature électronique :

- QuoVadis Trustlink Schweiz AG
- La Poste Suisse/SwissSign AG
- Swisscom (Suisse) SA
- Office fédéral de l'informatique et de la télécommunication (OFIT)

Le prix varie pour les utilisateurs privés entre 147 et 195 francs pour trois ans (La Poste ; SuisseID Signing Service/QuoVadis). Le service fonctionne avec une authentification par le biais d'une clé USB ou d'une carte à puce.

Le service SuisseID peut aussi être utilisé dans le cadre d'une authentification à des services en ligne et pourrait donc être utilisé dans le cadre de la Fédération FIDES.

3.4 Swisscom Mobile ID

Mobile ID est une identité numérique stockée sur la carte SIM d'un téléphone mobile (smartphone ou non). Le service est développé par Swisscom et est gratuit pour ses utilisateurs. Mobile ID est aussi disponible chez les opérateurs Sunrise et M-Budget et prochainement Salt. Mobile ID est une méthode d'authentification sécurisée pour accéder à des services utilisant ce type d'authentification. Le service est disponible à l'étranger, pour autant que le service SMS roaming soit activé. L'utilisation à l'étranger est aussi gratuite.

Bien que le service soit gratuit pour la création et l'utilisation de Mobile ID, certains fournisseurs peuvent facturer l'utilisation de Mobile ID pour accéder à leur service. Mobile ID peut aussi être utilisé dans le cadre d'une authentification à des services en ligne et pourrait donc être utilisé dans le cadre de la Fédération FIDES.

3.5 Fédération suisse d'identités (FSI)

3.5.1 Identités numériques et Cyberadministration suisse

Un projet stratégique du Secrétariat d'État à l'économie et de l'organisation Cyberadministration suisse. Cette stratégie de cyberadministration est commune à la Confédération, aux cantons et aux communes pour faciliter l'accès aux services administratifs de façon transparente et efficace et entièrement électronique pour la population suisse.

Le rôle du projet « Fédération suisse d'identités » est de développer les mesures organisationnelles nécessaires et l'infrastructure technique pour permettre à des systèmes d'identités d'être interconnectés. Par ailleurs, les utilisateurs pourront accéder à une multitude de services avec les mêmes moyens d'authentification.

Le projet prévoit une phase pilote au troisième trimestre de 2017 pour une finalisation au premier trimestre 2019.

3.5.2 Services

Applications locales de cyberadministration, vote électronique, déclaration d'impôts, mais aussi d'autres services car la fédération est bâtie sur un modèle ouvert. La Fédération FIDES pourrait donc bénéficier de ce projet. Les identités de la Fédération FIDES pourraient utiliser les services connectés à la FSI.

3.6 Office fédéral de la police fedpol

Le Conseil fédéral a chargé le Département fédéral de justice et police (DFJP) d'élaborer un concept et un projet de forme juridique pour le futur moyen suisse d'identification électronique (e-ID) proposé avec la nouvelle carte d'identité. Sur cette base, l'Office fédéral de la police (fedpol) a lancé une consultation informelle entre mai et juin 2015 sur un concept pour des systèmes d'e-ID suisses reconnus par l'Etat. Sur base de la consultation, ce concept a été révisé pour ouvrir la voie aux travaux sur la loi e-ID. Le 22 février 2017, le Conseil fédéral a mis en consultation la loi fédérale sur les moyens d'identification électroniques reconnus (loi e-ID).

3.6.1 Concept Fedpol

Le concept fedpol « Moyens d'identification électronique (e-ID) reconnus par l'Etat » prévoit que la Confédération ne publie pas ses propres e-ID mais s'appuie plutôt sur des solutions existantes sur le marché, tout en exerçant un rôle de surveillance et de reconnaissance par le biais d'un Organisme de reconnaissance des fournisseurs d'identité (ORFI) qui sera instauré.

Par ailleurs, la Confédération fait office de référentiel d'attributs (Attribute Repository) fiable pour l'identité des utilisateurs d'e-ID reconnus par l'Etat en transmettant par voie électronique des données d'identification personnelles. Une tâche qui incombera au Service d'identité électronique suisse (SIE) à mettre en place au sein des autorités fédérales.

3.6.2 Loi e-ID

La loi fédérale sur les moyens d'identification électronique reconnus par l'Etat (loi e-ID) vise à encadrer et garantir la sécurité du droit en matière d'e-ID. Elle règle les conditions des moyens d'identification électroniques reconnus, la reconnaissance et surveillance des fournisseurs d'identités (IdP), les droits et devoirs des titulaires d'un e-ID et ceux des fournisseurs de services (SP). Elle vise à promouvoir un espace de sécurité pour les transactions électroniques et à garantir la normalisation et l'interopérabilité des e-ID.

4 BONNES PRATIQUES DE FÉDÉRATIONS DES SERVICES D'IDENTITÉS DU DOMAINE SCOLAIRE DE PAYS EUROPÉENS

Il existe en Europe des fédérations d'identités pour le domaine scolaire. L'équipe de projet FIDES a été en contact avec plusieurs pays dans le but d'apprendre de leur expérience dans ce domaine et pour partager les spécificités du concept suisse pour une fédération des services d'identités.

Dans cette partie nous présentons certaines de ces fédérations, ce en quoi elles sont intéressantes au plan conceptuel, organisationnel, technique ou du point de vue de leur modèle d'entreprise. Les travaux sont principalement basés sur une rencontre et présentation de cinq projets nationaux de services d'identités pour le milieu scolaire qui s'est déroulée le 2 juin 2016 à Bruxelles en partenariat avec SwissCore et European Schoolnet. Cinq projets en provenance du Danemark, Estonie, France, Pays-Bas et Suisse ont été présentés. Nous en avons sélectionné trois ci-dessous.

La fédération Suédoise « Skolfederation », dont les représentants étaient présents lors de la réunion mais qui n'a pas fait l'objet d'une présentation, est aussi mentionnée ci-dessous pour son intérêt et similitudes avec le concept-cadre de la Fédération FIDES.

4.1 Danemark : UNI-Login

État : actif

Le système SSO par UNI-Login du ministère danois de l'enseignement, présente un exemple réussi d'accès pour les élèves à des services en ligne par le biais d'un login unique. Lancé il y a plus de 20 ans, le service a grandi pour compter aujourd'hui 350 000 login par jour sur des services variés tels que des ressources numériques en ligne, des intranets scolaires, des services en nuage ou des réseaux WIFI. Une nouvelle initiative « Portail Utilisateurs » vise à étendre le model UNI-Login à une gestion des accès standardisés aux services en ligne pour les écoles.

Le projet UNI-Login et sa suite « Portail Utilisateurs » est un bon exemple car :

- Il s'agit d'une fédération qui a démarré avec quelques IdP et SP et qui, par la suite, s'est agrandie, par opposition à un démarrage avec un grand nombre de parties prenantes dès le début.
- Les statistiques de connexion démontrent les besoins de flexibilité des systèmes techniques pour s'adapter à l'évolution de la demande et des infrastructures.

4.2 Estonie : HarID

État : en projet (phase de test)

La fédération « HarID » est un projet estonien pour fournir une identité digitale pour le personnel enseignant et pour les élèves de plus de 15 ans. Le service donnera accès par login SSO à plusieurs services en ligne au sein d'un nuage informatique estonien pour l'éducation (educcloud). Pour s'authentifier les élèves et membres du corps enseignant pourront utiliser leur carte d'identité nationale, leur téléphone portable ou autres services d'identité reconnus. La société estonienne est très en avance concernant la digitalisation des services comme la cyberadministration. Les données personnelles sur la base desquelles sont générées les identités numériques (HarID) pour les élèves et les enseignants se trouvant dans des bases de données nationales existantes (registre de la population et système national d'information sur l'éducation).

Le projet HarID est un bon exemple car :

- Utilisation de bases de données existantes pour générer les identités numériques. Une tendance que l'on observe dans plusieurs projets IdM cantonaux en Suisse.
- La mise en place d'un cloud pour l'éducation, sur la base de la fédération des services d'identités.

4.3 Pays Bas : Entree Federatie

État : actif

La fédération des services d'identités néerlandaise « Entree Federatie » pour le milieu scolaire aux Pays-Bas est gérée par Kennisnet, l'organisation publique pour ICT et l'éducation financée par le ministère de l'éducation, de la culture et des sciences. Dans le modèle actuel de la fédération « Entree », les écoles elles-mêmes peuvent demander leur entrée dans la fédération et peuvent choisir leur IdP. Celles-ci peuvent choisir entre quatre IdP, deux solutions privées et deux émanant du domaine public. Les SP en ligne signent un Service Level Agreement pour pouvoir participer à la fédération. Les écoles contrôlent quels attributs sont partagés avec les SP. En 2017 un nouveau système sera mis en place par lequel les élèves eux-mêmes peuvent choisir leur IdP, de plus l'authentification se fera sur la base d'une pseudoID anonymisée.

Le projet Entree Federatie est un bon exemple car :

- Coopération publique-privée dans le domaine des fournisseurs d'identités numériques
- Un Dashboard pour les écoles pour contrôler finement les attributs que leurs utilisateurs partagent avec les SP en ligne
- L'anonymisation des identités par le biais des pseudoID, un service que la Fédération FIDES souhaite aussi offrir en option (UUIDgen)
- Les coûts d'administration et de développement de la fédération néerlandaise peuvent orienter une estimation des coûts de la Fédération Suisse

4.4 Suède : Skolfederation

État : actif

En Suède, la fédération Skolfederation propose une solution de login SSO pour les élèves et les enseignants du milieu scolaire. Les municipalités, chargées de l'organisation des écoles sur leur district, ainsi que les écoles libres, collaborent avec les SP au sein de la fédération. Les SP doivent eux être parrainés par une municipalité ou école libre pour être admis dans la fédération. La gestion de la fédération est assurée par IIS, la fédération pour l'internet en Suède, une organisation indépendante.

Le projet Skolfederation est un bon exemple car :

- Le parrainage des SP pour entrer dans la fédération
- Le cercle de confiance mis en place par les différents contrats que les communes/écoles libres et les SP doivent conclure avant leur entrée dans la fédération