Guide sur les conditions et bonnes pratiques pour la mise en place d'une identité numérique nationale

Pôle d'expertise en cybersécurité
et impacts sociétaux de l'OBVIA

obvia

Août 2023

Crédits

Coordination et rédaction

Félix Gariépy, professionnel de recherche, Pôle d'expertise en cybersécurité et impacts sociétaux de l'OBVIA - Observatoire international sur les impacts sociétaux de l'IA et du numérique

Comité aviseur

- **Benoit Dupont**, Professeur à l'École de criminologie, Titulaire de la Chaire de recherche du Canada en cybersécurité et de la Chaire de recherche en prévention de la cybersécurité, Université de Montréal
- **Céline Castets-Renard**, Professeure à la Faculté de droit, Titulaire de la Chaire de recherche de l'Université sur l'intelligence artificielle responsable à l'échelle mondiale, uOttawa
- **Hugo Loiseau**, Professeur à l'École de politique appliquée, Membre du Groupe de recherche interdisciplinaire en cybersécurité, Université de Sherbrooke
- **Lyse Langlois,** Professeure au Département des relations industrielles, Directrice de l'Observatoire international sur les impacts sociétaux de l'IA et du numérique, Université Laval
- **Nadia Tawbi**, Professeure au Département d'informatique et de génie logiciel, Université Laval
- **Pierre-Martin Tardif**, Professeur à l'École de gestion, Membre du Groupe de recherche interdisciplinaire en cybersécurité, Université de Sherbrooke
- **Sébastien Gambs**, Professeur au Département d'informatique, Titulaire de la Chaire de recherche du Canada en analyse respectueuse de la vie privée et éthique des données massives, UQÀM
- **Steve Jacob**, Professeur au Département de science politique, Titulaire de la Chaire de recherche sur l'administration publique à l'ère du numérique, Université Laval

obvia

À propos de l'OBVIA

L'Observatoire sur les impacts sociétaux de l'IA et du numérique (OBVIA) est un réseau de recherche ouvert qui fédère les expertises de plus de 260 chercheuses et chercheurs. Au moyen d'une interrogation critique, l'OBVIA a pour mission d'identifier les enjeux sociétaux de l'IA et du numérique et de contribuer à des solutions qui placent les êtres vivants et la biosphère au centre de leur cycle de développement et d'utilisation. La communauté de recherche de l'OBVIA, en collaboration avec la société civile, les acteurs publics, l'industrie et les développeurs, produit des connaissances ouvertes et soutient le renforcement des capabilités individuelles et collectives.

À propos du Pôle d'expertise en cybersécurité et impacts sociétaux

Mis en place avec le soutien des Fonds de recherche du Québec et du Ministère de la cybersécurité (MCN), le Pôle d'expertise en cybersécurité et impacts sociétaux repose sur des expertises de chercheuses et chercheurs de l'OBVIA et vise la mise en place de diverses activités et initiatives de recherche répondant aux besoins et priorités des partenaires gouvernementaux et d'autres milieux preneurs afin de renforcer le leadership et les capacités de recherche, de veille et de formation en cybersécurité au Québec.

ISBN : 978-2-925138-32-7 DOI : 10.61737/AFQC2028

Table des matières

RÉSUMÉ

Ce guide poursuit deux objectifs, soit (1) le développement des connaissances sur les conditions et bonnes pratiques pour la mise en place d'une identité numérique nationale ainsi que (2) la mise en évidence dans une perspective critique des enjeux, impacts et conséquences envisageables de l'implantation d'un projet d'identité numérique nationale sur la société, les organisations et les individus. L'étude de cette question s'inscrit dans la mission plus large du **Pôle d'expertise en cybersécurité et impacts sociétaux** de *l'Observatoire international sur les impacts sociétaux de l'intelligence artificielle et du numérique (OBVIA)* d'alimenter la recherche sur la cybersécurité au Québec considérant que l'identité numérique a pour objectif d'assurer les principes fondamentaux de la sécurité de l'information, notamment par la protection des renseignements personnels.

Divisé en deux sections, la première partie du Guide dresse une revue de la littérature en lien avec les défis liés à la mise en place d'une identité numérique gouvernementale en plus d'aborder rapidement les différentes formes que peuvent prendre les systèmes de gestion de l'identité numérique. De cette première partie, nous retenons que les principaux défis sont en lien avec (1) la gouvernance, (2) la gestion et l'organisation, (3) les lois et les normes, (4) l'adoption et finalement, (5) les défis liés à la technologie. La seconde partie se veut quant à elle être une étude de cas de plusieurs États (Royaume-Uni, Estonie, Australie, Suède, Singapour, Finlande et Danemark). L'importance de l'utilité perçue par la population pour le succès d'une identité numérique nationale représente le principal constat de cette partie. La proposition de pistes d'action conclut le présent Guide.

CONTEXTE HISTORIQUE

C'est au début des années 2000 que le Gouvernement du Québec annonce sa volonté de développer le gouvernement en ligne québécois, notamment à travers le plan de modernisation de l'État québécois *Moderniser l'État: Pour des services de qualité aux citoyens* publié en 2004. Inspiré du mouvement managérial de la Nouvelle gestion publique, le développement du gouvernement en ligne québécois s'appuyait sur « l'idée que le développement d'un gouvernement en ligne fondé sur les TI permettrait de rationaliser la prestation de services et la rendre plus efficace et ce, à moindre coût » (Gariépy, 2023, 35). Parallèlement, ce développement alla de pair avec la nécessité des différents gouvernements de pouvoir authentifier de manière sécuritaire la population dans le cas de prestation de services ou de transactions en ligne. Plus récemment, la volonté d'élargir l'offre de services en ligne avec, par exemple, SAAQclic, sans oublier la pandémie qui a été un élément déterminant, n'a fait que souligner ce besoin.

L'émergence des premiers systèmes de gestion de l'identité numérique gouvernementale (SGING)[1] apparaissent dans cette lignée de modernisation technologique, soit à la fin des années 1990, et connaissent des succès mitigés (OCDE 2011). À titre d'exemple, les SGING singapourien et estonien jouissent d'une forte adoption par la population et sont largement considérés comme des succès tandis que d'autres États, dont l'Australie et le Royaume-Uni, ont eu moins de succès. Peu d'études nous permettent cependant de comprendre les facteurs ayant contribué au succès ou à l'échec de ces SGING. Pour de nombreuses raisons, l'étude de cette question est aussi pertinente sur le plan social que scientifique, d'autant plus que les SGING ont pour objectifs d'assurer les principes de base de la cybersécurité (disponibilité, intégrité, authentification et confidentialité).

Au niveau social, plusieurs gouvernements, dont celui du Québec avec le *Service québécois d'identité numérique*, sont actuellement en train de développer des SGING. En ce sens, l'étude des différents facteurs de succès permettrait de faciliter la transformation numérique des États. De plus, une telle étude aurait le mérite de mettre en lumière les différents enjeux et risques en lien avec le développement des SGING. Finalement, il importe de se pencher sur la dimension sociale des SGING (ex. gouvernance, lois et normes, etc.) considérant son importance, surtout qu'elle fut longtemps négligée au détriment des aspects techniques de l'identité numérique malgré le fait qu'ils soient interreliés (Alkhalifah, 2013). Sur le plan scientifique, l'étude de cette question permettrait de nourrir le peu de connaissances sur le sujet en plus de développer les connaissances ne relevant pas d'une approche technocentriste. De plus, la littérature scientifique à cet égard remonte majoritairement au début des années 2010.

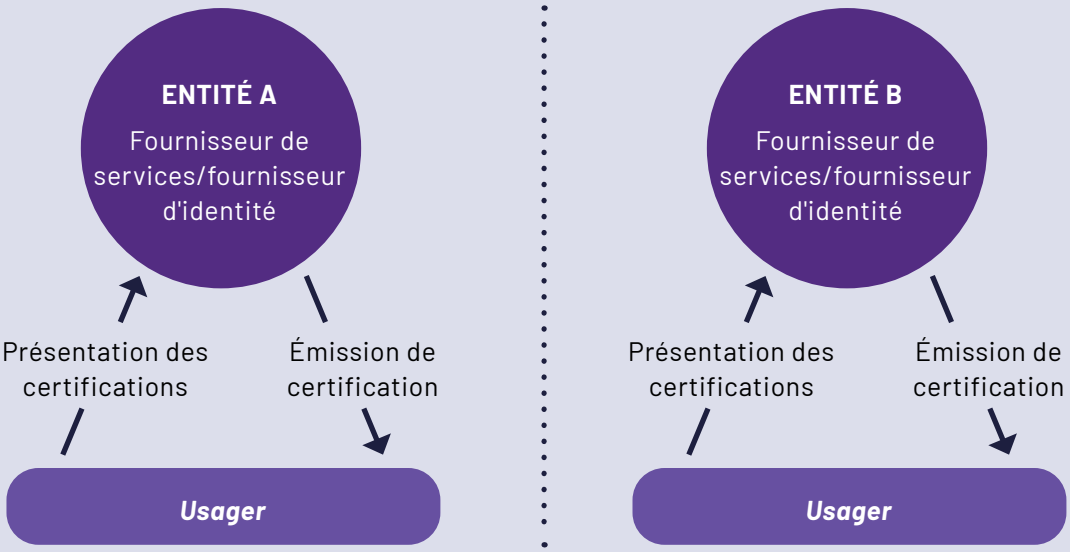
Dans cette optique, il importe de déterminer les bonnes pratiques en lien avec la mise en place d'un SGING afin de faciliter la transformation numérique du gouvernement du Québec et des autres gouvernements. Pour ce faire, nous brosserons un portrait de la littérature scientifique sur le sujet dans l'objectif de déterminer les facteurs de succès d'un SGING. Finalement, nous offrirons une présentation de SGING de différents États dans le but d'en tirer des leçons. Ces États ont été sélectionnés sur la base de certains éléments, dont l'ancienneté du SGING, l'implication du gouvernement ainsi que les bonnes et mauvaises pratiques.

1 Les systèmes de gestion de l'identité numérique gouvernementale font référence à des ensembles de « procédés, de politiques et de technologies émergentes visant la création, la maintenance et l'utilisation d'identités numériques [et de ses attributs] sur Internet et au sein des fournisseurs de services » (Alkhalifah, 2013, 25) dans un contexte gouvernemental.

MODÈLES DE SYSTÈMES DE GESTION DE L'IDENTITÉ NUMÉRIQUE GOUVERNEMENTALE (SGING)

Avant d'entrer dans le vif du sujet, il convient de présenter préalablement les différents modèles de SGING afin de faciliter la compréhension de l'ensemble du document. De manière générale, nous distinguons trois modèles présentant chacun des avantages et des désavantages, soit le modèle isolé, le modèle fédéré ainsi que le modèle décentralisé. Ces différents modèles s'inscrivent au sein de l'évolution des SGING permettant de répondre aux besoins engendrés par le changement du cyberespace au cours des dernières décennies. D'une part, nous retrouvons le modèle isolé, soit la première génération d'identité numérique, où le fournisseur de service occupe également le rôle de fournisseur d'identité. Alors que ce modèle est relativement facile à mettre en place, il présente plusieurs inconvénients, dont une centralisation des données, une absence d'interopérabilité ainsi qu'un grand nombre de mots de passe à retenir. Ce dernier élément est cependant remis en question vu la généralisation des gestionnaires de mots de passe dans les dernières années. De plus, l'accroissement des services en ligne nécessitant une authentification des individus a rendu son usage excessivement compliqué pour les usagers en plus d'être redondant.

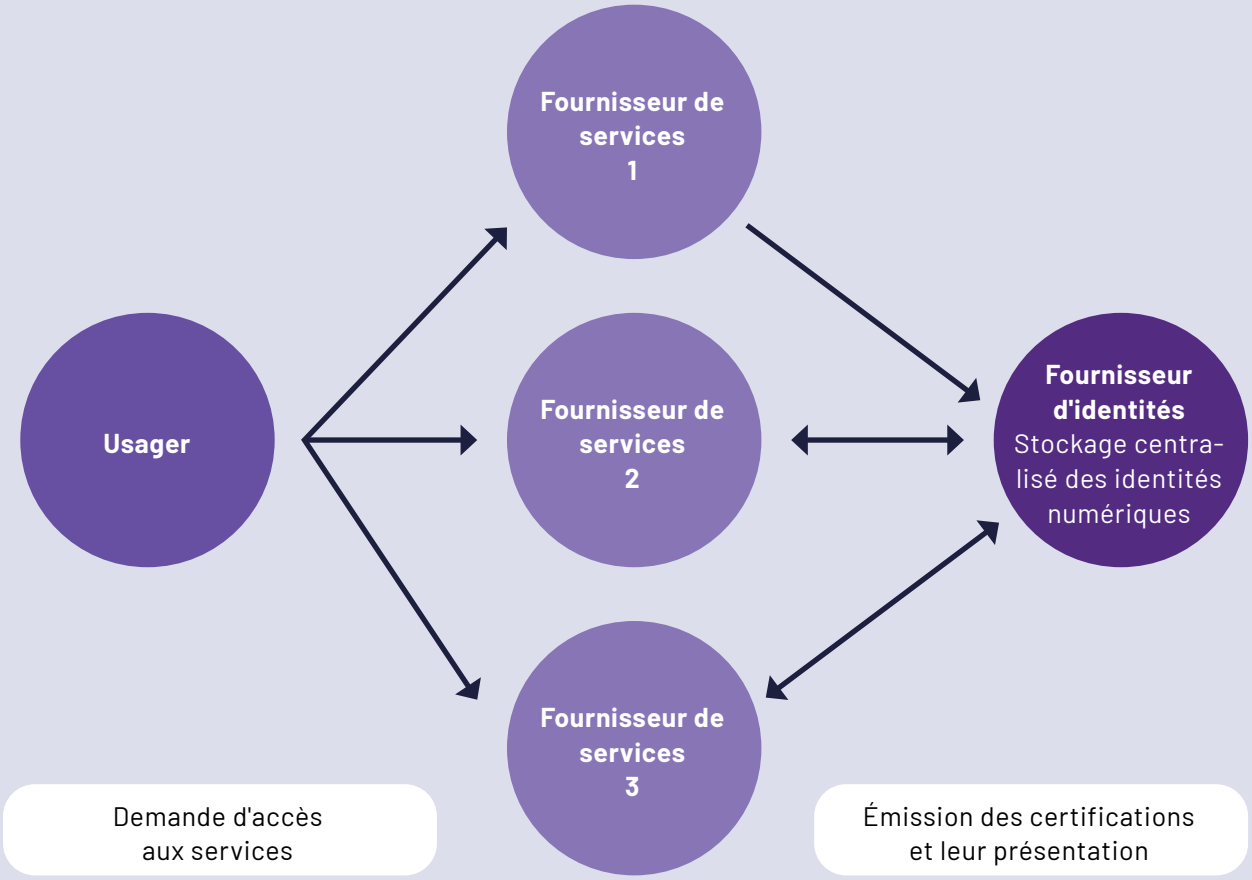
Figure 1 - Modèle isolé



Félix Gariépy (2023)

Le modèle fédéré fut donc développé en réponse au besoin de faciliter le processus d'authentification en permettant l'accès à plusieurs fournisseurs de services par le biais d'un seul fournisseur d'identités. Autrement dit, il est possible au sein du modèle fédéré d'accéder à plusieurs services en ligne par le biais d'une seule identité numérique (authentification unique ou *Single sign-on*). Si le modèle fédéré se distingue du modèle isolé par son interopérabilité, il présente certaines vulnérabilités et enjeux de vie privée en raison de la centralisation des données personnelles au sein d'un seul fournisseur d'identités. Autrement dit, la sécurité des différents services est compromise dès lors qu'une personne malintentionnée a accès aux informations d'identification d'un usager.

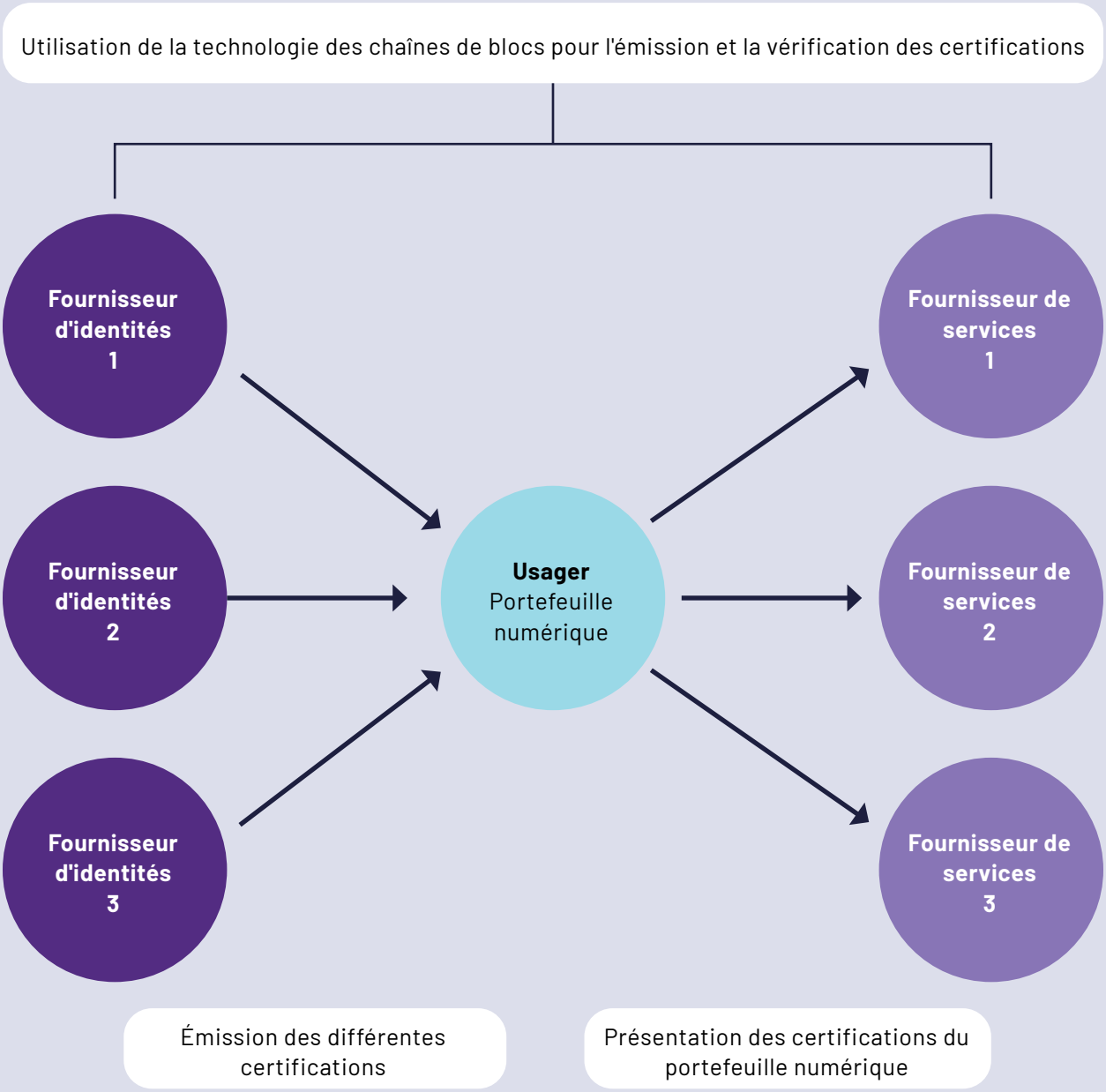
Figure 2 - Modèle fédéré



Félix Gariépy (2023)

Nous retrouvons finalement le modèle décentralisé qui émergea avec le développement de la chaîne de blocs. Ce modèle peut se définir par son objectif, soit de « permettre aux individus de contrôler leurs différentes identités [...] et d'avoir les outils pour contrôler le flux de leurs données personnelles dans les transactions » (Avellaneda *et al.*, trad., 2019, 11). Pouvant notamment prendre la forme de portefeuilles numériques, le modèle décentralisé est organisé autour des notions de consentement et de contrôle des individus.

Figure 3 - Modèle décentralisé



Félix Gariépy (2023)

REVUE DE LA LITTÉRATURE

Dans l'objectif de déterminer les bonnes pratiques en lien avec la mise en place d'un SGING, nous nous inspirerons de la terminologie développée par Gil-García et Pardo (2005) ayant pour objectif de catégoriser les défis et les enjeux en lien avec les projets de gouvernement en ligne ainsi que celle développée par Pöhn et al. (2021) qui concerne directement les SGING. L'usage de ces terminologies est motivé par le fait que l'identification des défis permet à la fois de déterminer les freins et les éléments de succès dans la mise en place d'un SGING. De manière parallèle, nous aborderons les risques associés aux SGING.

Défis et enjeux

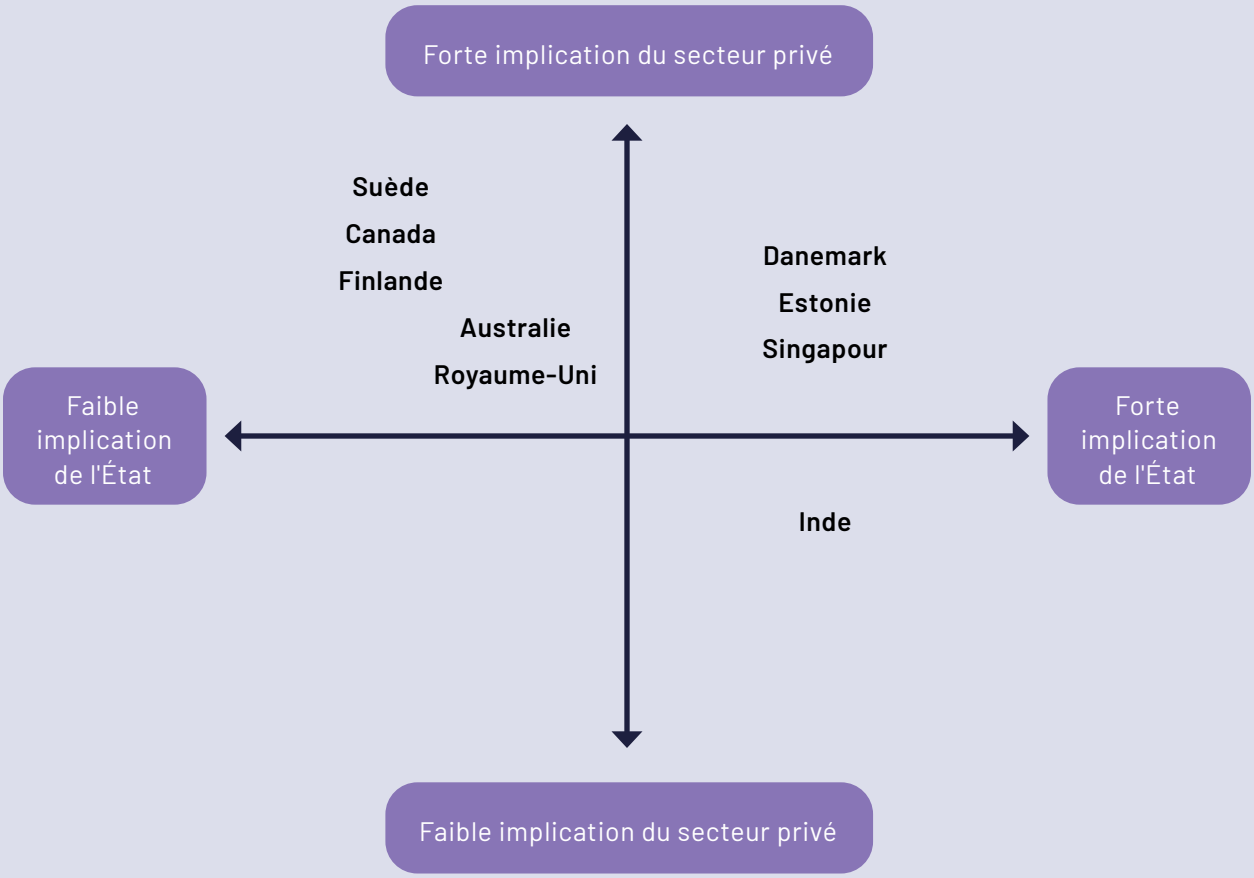
Les catégories de défis qui seront abordés sont les suivantes : (1) les défis liés à la gouvernance interorganisationnelle (2) les défis liés à la gestion et l'organisation, (3) les défis liés aux lois et normes, (4) les défis liés à l'adoption et finalement, (5) les défis liés à la technologie. Par ailleurs, si ces ensembles de défis sont abordés de manière séparée, il importe de les comprendre comme un tout étant donné la manière dont ils sont liés les uns aux autres.

Défis liés à la gouvernance

Comme le souligne l'Union internationale des télécommunications (2018), le type de gouvernance au sein d'un SGING varie en fonction du degré d'implication du gouvernement. Celle-ci varie sur un spectre allant d'une faible implication, ce qui peut se traduire par le simple rôle de régulateur (ex. Canada avec le système *SecureKey Concierge*[2]) jusqu'à une forte implication de l'État où par exemple, celui-ci occupe le rôle de fournisseur d'identités (ex. Estonie et Singapour). Dans le même sens, cette gouvernance varie également en fonction de l'implication du secteur privé. Cela étant, chaque combinaison de degré d'implication de ces acteurs présente des avantages et des inconvénients. À titre d'exemple, une gouvernance où l'État est fortement impliqué et où le secteur privé est tout autant impliqué a généralement pour avantage de donner lieu à des SGING largement adoptés par la population, notamment vu les cas d'utilisations importants. Au contraire, la gestion de certaines données personnelles par le secteur privé peut présenter des enjeux de vie privée.

2 Le système SecureKey Concierge est un courtier de crédits permettant de se connecter aux services gouvernementaux en ligne canadiens par le biais de ses informations bancaires.

Figure 4 - Classification des SGING en fonction de l'implication des différents acteurs gouvernementaux et privés



Félix Gariépy (2023)

Indépendamment du niveau d'implication du gouvernement au sein d'un SGING, la question de la gouvernance interorganisationnelle est primordiale puisque ce type de projet requiert l'implication de plusieurs agences gouvernementales et organisations du secteur privé dans certains cas.

D'emblée, il fut constaté que le manque de coordination et de coopération représenta un frein au développement de SGIN gouvernementaux dans plusieurs États européens (Melin et al., 2016, p. 7). En ce sens, des chercheurs mettent de l'avant **l'importance de la présence d'une autorité centrale gouvernementale (ex. *Digital Transformation Agency* en Australie) assurant une coordination et une coopération entre les différentes agences gouvernementales afin de s'assurer d'une communication entre leurs bases de données, d'une certaine uniformité dans le déploiement d'un SGING et finalement, d'éviter un dédoublement des systèmes** (Melin et al., 2016). Au Québec, la concentration des activités liées à la cybersécurité et au numérique, dont le *Service québécois d'identité numérique*, au sein du ministère de la Cybersécurité et du Numérique (MCN) vise notamment à faciliter la coordination de ces activités. Par ailleurs, il peut parfois s'avérer nécessaire d'adopter des lois ou règlements facilitant cette coopération ou cette coordination. À titre d'exemple, la création du MCN et la *Loi favorisant la transformation numérique de l'administration publique* visent justement à faciliter, voire rendre possible, cette coopération et cette coordination nécessaires entre différentes agences gouvernementales du Québec.

Dans le même ordre d'idées, l'absence d'une autorité de coordination centrale fut notée comme étant problématique lors du développement de l'identité numérique nationale en Suède au début des années 2000 (Melin et al., 2013, 7). Une gouvernance de type verticale avec une autorité centrale serait davantage gage de succès qu'une gouvernance de type horizontale où les agences gouvernementales jouissent d'une plus grande autonomie. De plus, il importe que cette gouvernance soit accompagnée d'une vision claire du SGING pour guider les différents acteurs impliqués (Union internationale des communications, 2018). Dans le cas où le secteur privé est impliqué, la question de la gouvernance est tout aussi importante pour définir les rôles, les besoins, et les choix technologiques ainsi que pour assurer le respect des lois et des normes (Banque mondiale, 2016).

Défis liés à la gestion et l'organisation

De manière évidente, les défis associés à la gestion et l'organisation des SGING sont cruciaux en ce qui a trait au succès de ces derniers. D'emblée, Melin et al. (2013) expliquent que la taille du projet ainsi que la diversité des acteurs impliqués représentent les principaux défis de cette catégorie. En ce sens, Gil-García et Pardo (2005) proposent d'adopter des objectifs réalistes et clairs en fonction des ressources disponibles en plus d'impliquer les acteurs concernés, dont la population et les organismes représentant la société civile. Par ailleurs, le fait d'impliquer la population dans le développement d'un SGING permettrait aux gouvernements de mieux comprendre les attentes de la population, de justifier l'utilisation d'un tel système et ultimement, de diminuer certains risques associés à une faible acceptabilité sociale. **De manière plus large, l'implication des acteurs concernés, dont les différentes organisations gouvernementales et dans certains cas le secteur privé, pourrait permettre d'aligner les attentes et les objectifs de ces derniers dans l'optique de développer une solution convenant au plus grand nombre d'acteurs (Banque mondiale, 2016).**

Manifestement, il importe d'avoir les ressources nécessaires au développement d'un SGING, dont celles d'ordre technique, faute de quoi il peut s'avérer nécessaire d'engager davantage de personnel qualifié ou d'avoir recours au secteur privé par le biais de la sous-traitance ou de partenariats public-privé (PPP)[3]. Concernant la sous-traitance, les principaux arguments mis de l'avant pour justifier ce choix dans un contexte de projet informatique sont souvent le manque de personnel qualifié au sein du secteur public et de ressources financières (Perry et Chen, 2016; Yang et al., 2008). En dépit des bénéfices avancés, soulignons que la sous-traitance en informatique au Québec n'a pas tout le temps permis d'atteindre les objectifs désirés, en plus de poser un risque de dépendance envers le secteur privé comme le note un rapport du Vérificateur général du Québec (2012).

De manière plus spécifique au mode de gestion des PPP, les principaux arguments en sa faveur d'un point de vue gouvernemental consistent en une réduction des coûts, un partage des risques, l'accès à une expertise que le gouvernement n'a pas nécessairement et dans certains cas, l'avantage de profiter de SGIN avec une clientèle établie (ex. les SGIN utilisés par les institutions financières). Cependant, certains auteurs soulèvent certains risques associés aux PPP dont la dépendance des gouvernements envers le secteur privé additionnés de craintes quant à la protection de la vie privée dans un contexte de monétisation des données et d'une croissance des incidents de cybersécurité (Mettler et Guenduez, 2019; Abraham, 2020). Qui plus est, mentionnons que les missions respectives de l'État et du secteur privé peuvent être en contradiction considérant les finalités poursuivies qui ne sont pas les mêmes.

3 Un PPP, qui est une forme de sous-traitance, est un « contrat à long terme par lequel une entreprise du secteur public associe une entreprise du secteur privé, avec ou sans financement de celle-ci, à la conception, à la réalisation et à l'exploitation d'un ouvrage public. Un tel contrat peut avoir pour objet la prestation d'un service public. » (Loi sur l'agence des partenariats public-privé du Québec, 2010).

En dépit des débats entourant la sous-traitance et les PPP, soulignons que dans la plupart des États, on note une implication du secteur privé à divers degrés dans les SGING. Comme le mentionnent Yang et al. (2008), la sous-traitance peut se faire en lien avec le développement ou la maintenance du système. À titre d'exemple, l'Estonie relégua au secteur privé, au début des années 2000, le développement de la technologie X-Road[4] qui est le pilier de son SGING.

Dans le même ordre d'idées, tant le type de PPP que l'ampleur de celui-ci peuvent varier d'un État à l'autre. Alors que les types de PPP peuvent prendre la forme d'ententes de services ou de concessions, l'ampleur de ceux-ci varie au niveau de l'implication du secteur privé en lien avec (1) le financement du SGING, (2) la conception et le développement de celui-ci et finalement (3), les opérations au sein du SGING (ex. à titre de fournisseur d'identités ou de services) (Banque mondiale, 2016). À titre d'exemple, la Suède opta pour un modèle où le gouvernement met en place le cadre réglementaire alors que certaines organisations, dont le consortium de banques *BankID*, s'occupent essentiellement du développement du SGING et des opérations au sein de celui-ci, ce qui comprend notamment l'émission de certifications (Grönlund, 2010). **Cependant, comme le soulignent Medaglia et al. (2017) l'exemple du Danemark au regard d'une identité numérique nationale n'a été possible qu'à partir d'une convergence des ressources, d'intérêts communs et d'une gouvernance entre les secteurs privés et publics.**

Défis liés aux lois et normes

Que ce soit pour des raisons de protection de la vie privée ou pour des raisons de faisabilité, il est impératif que le développement de SGING, et les projets de gouvernement en ligne se fassent conjointement avec l'adoption de normes et de lois encadrant cette transformation numérique. À titre d'exemple, plusieurs États et organismes adoptèrent au début des années 2000 des cadres réglementaires pour encadrer les signatures électroniques, dont la directive de l'Union européenne 1999/93/EC[5] (Medaglia et al., p. 2785). Au Québec, on pense notamment à la récente *Loi favorisant la transformation numérique de l'administration publique* qui facilite la communication et l'utilisation des renseignements personnels des organismes publics pour des projets informatiques d'intérêt gouvernemental ainsi que la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* ayant pour objectif d'encadrer l'utilisation et la protection des données personnelles au sein des organisations québécoises.

Par ailleurs, l'absence ou l'insuffisance de telles lois encadrant les SGING et la sécurité/le traitement des données peuvent représenter un risque important pour la vie privée de la population. À titre d'exemple, le système Aadhaar du gouvernement indien, l'un des plus grands au monde, a été déployé en 2010 sans cadre réglementaire étoffé relatif à l'usage de cette identité numérique ou à la protection des renseignements que contient celle-ci et a entrainé des dérives importantes pour les individus. L'absence d'un tel cadre a eu pour effet d'élargir l'usage de cette identité numérique, notamment aux secteurs bancaires ou médicaux alors qu'elle concernait initialement l'aide gouvernementale. Cet élargissement semble s'être fait au gré des opportunités sans véritablement de planification (Dixon, 2017, 542-543).

4 X-Road est un logiciel facilitant l'échange de données entre les secteurs privés et publics de la société estonienne.
5 Cette réglementation a été remplacée en 2014 par la réglementation eIDAS (Règlement UE no.910/2014).

Dans le même sens, l'absence de cadre réglementaire pose un risque de concentration des pouvoirs de surveillance de l'État et par le fait même, d'usages illicites du système Aadhaar (Sen, 2019, p. 3). **Ultimement, si cette absence ou insuffisance présente des risques sociopolitiques et relatifs à la protection de la vie privée, elle peut également miner la confiance des acteurs envers le système, influençant par le fait même l'adoption de ce dernier (Banque mondiale, 2016**). En ce sens, l'existence d'une autorité indépendante supervisant le respect des normes et des lois, s'assurant notamment de la protection efficace des données personnelles, est primordiale pour assurer la confiance de la population envers le système (OECD, 2021, 24). Par ailleurs et pour faire un pont avec la section précédente sur la gouvernance, il importe que cette autorité dispose de ressources suffisantes pour effectuer ce travail de surveillance.

Dans un autre ordre d'idées, l'adoption d'un cadre réglementaire et législatif adapté est d'autant plus importante considérant le rôle qu'occupe le secteur privé dans la majorité des SGING via les PPP et la sous-traitance (Lips, 2010, 282-286). Pratiquement tous les pays analysés dans ce rapport ont procédé à cette adoption ou modification réglementaire. Qui plus est, soulignons que le caractère dématérialisé du cyberespace et l'extraterritorialité de certaines lois (ex. CLOUD Act) ne font qu'exacerber le besoin de réformes réglementaires et législatives dans un contexte où le secteur privé occupe une place importante.

Défis liés à l'adoption

Comme l'expliquent Gil-García et Pardo (2005), la technologie utilisée dans le cadre d'un projet de gouvernement en ligne, dont un SGIN gouvernemental, a un impact sur l'adoption de ce dernier, et donc sur son succès. En effet, une technologie avec laquelle une population n'est pas à l'aise ou ne perçoit pas les bénéfices représentera un frein à l'adoption d'un SGING. Au tout début de l'établissement de l'identité numérique nationale danoise, le peu de bénéfices perçus et les difficultés techniques ont représenté des obstacles à l'adoption de l'identité numérique nationale (Eaton et al., 2018, p. 74). Par ailleurs, le fait de rendre un SGING obligatoire n'est pas garant d'une forte utilisation en plus de comporter des risques politiques (Banque mondiale, 2018). Aussi, l'adoption de politiques « numérique par défaut » comporte plusieurs risques en dépit du fait qu'elles ont pour objectif de favoriser l'adoption des SGING. Parmi ceux-ci, notons que ce type de politique peut se faire au détriment de la prestation de services en personne en plus d'être considéré comme déshumanisant par certains (Ngwenyama, Henriksen, et Hardt, 2021). De plus, ces politiques risqueraient d'accentuer le fossé numérique au sein de la population et les inégalités sociales par le fait même, puisque les technologies ne représentent plus une commodité, mais davantage une nécessité dans ce contexte. En ce sens, il importe d'accompagner ce type de politique de mesures visant la démocratisation des technologies de l'information et de leur usage afin d'en atténuer les effets pervers.

De manière plus large, il fut constaté que l'utilité perçue, la facilité d'utilisation perçue, la protection de la vie privée perçue ainsi que la confiance perçue avaient un impact sur l'adoption d'un SGING (Adjei et Olesen, 2011). **À cet égard, plus une identité numérique peut être utilisée quotidiennement, plus sa valeur augmente aux yeux de la population (OCDE, 2021).** La facilité d'utilisation perçue est tout aussi importante comme le démontrent les difficultés rencontrées par les utilisateurs de la plateforme SAAQclic lors du déploiement de cette dernière. La confiance envers les institutions et l'importance accordée à la vie privée occupent également une place importante dans l'adoption d'un SGING. De plus, le choix de certains modèles de SGIN s'appuyant sur des protocoles et des technologies différentes a un impact sur le succès d'une identité numérique nationale. En effet, alors que certains modèles sont plus simples, d'autres permettent un plus grand contrôle des usagers sur leurs données tandis que d'autres modèles sont réputés comme étant plus sécuritaires. Qui plus est, certains défis culturels et sociaux doivent également être considérés dans la mise en place d'un SGING. À titre d'exemple, certains États sont déjà familiers avec le concept d'identité nationale (ex. les pays nordiques ou la France) tandis que d'autres n'ont pas de tels documents pour des raisons historiques ou personnelles (ex. États-Unis). Dans cette optique, l'arrimage de l'identité numérique nationale sur un document d'identification répandue pourrait réduire certains risques liés à la nouveauté que représente une identité numérique nationale (Bernat, 2011).

En ce sens, les autorités jouent un rôle primordial dans la communication des objectifs et des motifs justifiant la mise en place d'une identité numérique nationale. L'implication des acteurs concernés, dont la société civile, dans le processus, permettrait donc de faciliter cette communication tout en répondant aux craintes et questions, d'autant plus que c'est la société civile qui est l'utilisatrice principale des identités numériques nationales.

Défis liés à la technologie

Bien que les éléments non-techniques d'un SGING soient cruciaux, les défis techniques ne sont pas pour autant à négliger puisqu'ils contribuent directement à la confiance accordée par les utilisateurs envers le SGING. En ce sens, nous nous concentrerons sur la sécurité des SGING, dont les éléments relatifs à l'authentification.

Comme le souligne l'OCDE (2021, trad., 20), « le niveau d'assurance approprié est jugé en fonction de l'équilibre entre la réduction des risques et la facilité d'utilisation ». À cet égard, ce choix se fait notamment en fonction du risque de fraude et des conséquences qu'occasionnerait un tel événement (OCDE, 2021). Autrement dit, plus les risques et les conséquences sont élevés, plus le niveau d'assurance doit être élevé. Ainsi, le SGING doit prendre en compte le type de services rendus par le biais de ce dernier dans sa conception faute de quoi le SGING pourrait être difficile d'utilisation par rapport aux risques réels ou être insuffisamment sécuritaire. À titre d'exemple, le Canada divise les niveaux d'assurance en quatre niveaux en fonction des risques et des conséquences que pose un compromis des données. Plus le niveau est élevé, plus les critères sont élevés en ce qui a trait à l'évidence de l'identité, l'exactitude des informations ainsi que le lien entre l'information et l'individu (Gouvernement du Canada, 2016).

D'un autre côté, certains auteurs ne mettent pas les concepts de sécurité et de facilité d'utilisation en opposition, mais plutôt comme étant conciliables à travers la protection de la vie privée dès la conception (*Privacy by Design*). À cet égard, une plus grande protection de la vie privée, additionnée d'un certain contrôle sur ses données personnelles, influencerait de manière positive l'expérience des utilisateurs (OCDE, 2021). En ce sens, différents modèles de SGING, dont les modèles fédérés et décentralisés, faciliteraient le contrôle des individus sur leurs données en plus d'éviter la concentration de celles-ci au sein d'une base de données centrale.

De manière générale, nous distinguons trois méthodes d'authentification fondées sur ce que nous savons (ex. mot de passe), sur ce que nous sommes (ex. reconnaissance faciale) ainsi que sur ce que nous possédons (ex. carte physique). Chacun de ces moyens d'authentification comporte des avantages et des désavantages. Par exemple, alors que les noms d'utilisateurs et les mots de passe sont faciles d'utilisation, ils ne sont pas réputés sécuritaires comparativement à d'autres méthodes en raison de l'utilisation du même mot de passe pour plusieurs applications. Par ailleurs, soulignons que l'utilisation des différents moyens d'authentification n'est pas mutuellement exclusive et que la combinaison de plusieurs facteurs d'authentification est réputée comme étant davantage sécuritaire (OCDE, 2021). Cependant, rappelons que la sécurité d'aucun SGING n'est infaillible et que l'utilisation de technologies sophistiquées (ex. biométrie, chaîne de blocs) n'est pas garante en soi de la sécurité d'un système.

En plus de s'assurer d'un mécanisme d'authentification facilement utilisable et fiable, les organismes qui adoptent l'identité numérique pour accéder à leurs services doivent se doter de mécanismes de vérification et de certification de toutes leurs applications utilisant les identités numériques pour empêcher les fuites de données. Des mécanismes de détection d'intrusion doivent être toujours actifs pour empêcher les intrusions malveillantes. La résilience et la tolérance aux pannes des mécanismes d'identification doivent être pensées dès les premières phases de conception. Autrement dit, s'il y a panne matérielle, défaut logiciel ou intrusion, le système devrait pouvoir continuer à fonctionner.

ÉTUDE DE CAS: 7 EXEMPLES DE SGING

Cette section a pour but de présenter le développement d'identités numériques nationales au sein de sept États, soit le Royaume-Uni, l'Estonie, l'Australie, la Suède, Singapour, la Finlande et le Danemark dans l'objectif d'en tirer des leçons.

De manière plus concrète, nous aborderons les modèles de chacun des pays, les défis auxquels ils ont fait face ainsi que les défis de succès de chacun. Plusieurs éléments justifient le choix de ces États à titre d'étude de cas. D'emblée, le Royaume-Uni et l'Australie furent sélectionnés en raison de leur ressemblance avec le Canada. De plus, le cas britannique a le mérite de mettre en lumière les éléments représentant un frein au développement et l'adoption d'un SGING.

Ensuite, Singapour et l'Estonie furent choisis puisqu'ils sont reconnus comme étant parmi les SGING les plus développés au monde. Ces cas nous permettront d'identifier les différentes pratiques ayant permis de développer un SGING jouissant d'un large succès.

Finalement, la Suède, la Finlande ainsi que le Danemark ont été choisis parce qu'ils furent parmi les premiers États à développer des SGING et constituent une source d'apprentissage intéressante. De plus, ils permettent de mettre en lumière le fonctionnement et les motivations d'un système où le gouvernement occupe davantage le rôle de régulateur plutôt que de développeur. En ce sens, ils illustrent également le rôle important que peut jouer le secteur privé au sein d'un SGING.

Royaume-Uni

Le gouvernement britannique lança en 2016 le système *GOV.UK Verify* avec pour objectif de créer un système permettant d'accéder aux services gouvernementaux de manière sécuritaire. Qui plus est, cette identité numérique nationale, qui se base sur le modèle fédéré, se fit en partenariat avec cinq fournisseurs d'identités issus du secteur privé chargé de valider l'identité des individus. Cependant, trois ans après son lancement, *Verify* n'avait toujours pas rempli ses objectifs en plus d'avoir été faiblement adopté tant par les agences gouvernementales que par la population. Pour reprendre les termes d'un rapport de la Chambre des communes de Londres, ce projet « démontre plusieurs échecs récurrents des grands projets gouvernementaux : des attentes trop élevées, les différents objectifs n'ont pas été atteints et les services attendus n'ont pas été livrés » (Committee of Public Accounts, trad., 2019). En effet, alors que le gouvernement prévoyait 25 millions d'utilisateurs en 2020 et une utilisation par plus de 46 agences gouvernementales, seulement 19 agences avaient adopté ce dispositif en 2020 en plus d'être utilisé par seulement 3.9 millions de personnes. À cet égard, (1) le manque d'incitatifs pour les agences gouvernementales d'intégrer *Verify*, (2) les coûts d'implémentation pour les agences, (3) les problèmes de compatibilité avec les systèmes existants, (4) le manque de collaboration, (5) l'absence d'un plan clair et (6) le manque de leadership apparaissent comme la source du problème. Dans un autre ordre d'idées, on note également l'existence de problèmes en lien avec l'inscription des individus à *Verify*. En effet, près de la moitié des personnes ayant voulu s'inscrire au système n'ont pas été en mesure de le faire du premier coup. L'ensemble de ces problèmes aboutit à l'abandon du système d'identité numérique *Verify* en 2022. Depuis cet échec, le gouvernement britannique travaille en partenariat avec le secteur privé à l'élaboration d'une nouvelle identité numérique nommée *One Login* (Government Digital Service, 2023).

Estonie

C'est en 1997 que le gouvernement estonien entama les travaux en lien avec le développement d'un document d'identité nationale électronique. Rapidement, des partenariats avec le secteur bancaire et celui des télécommunications furent conclus pour développer cette identité numérique qui a été rattachée à la carte d'identité nationale obligatoire. Qui plus est, le gouvernement entreprit des réformes législatives et réglementaires pour permettre cette transformation, notamment en encadrant les signatures électroniques. En 2002, la première carte d'identité contenant une identité numérique a été émise.

Parmi les raisons expliquant le succès de cette identité numérique nationale, Martens (2010) note la forte implication du secteur privé par la société SK et la collaboration entre le gouvernement et les acteurs privés. En effet, cette implication favorisa l'adoption de cette identité par le secteur privé (ex. pour accéder aux services bancaires en ligne). Autrement dit, elle créa les incitatifs nécessaires à l'adoption de cette identité. Par ailleurs, le lancement d'une version mobile de cette identité favorisa son adoption, notamment en ce qui a trait à la facilité d'utilisation perçue.

De manière plus générale, l'identité numérique nationale estonienne s'intègre dans le projet plus large du gouvernement en ligne estonien fonctionnant sur la technologie X-Road[6] et sur la technologie de la chaîne de blocs depuis 2008. À titre d'exemple, les services gouvernementaux offerts en ligne comprennent notamment le vote en ligne ainsi que la numérisation du système de santé (E-Estonia, 2023). À cet égard, soulignons que cette transformation numérique ne se fit pas sous l'égide d'une autorité centrale, mais plutôt suivant une gouvernance horizontale où les différents organismes sont responsables de leur transformation numérique respective. Le gouvernement estonien a misé sur l'interopérabilité des données des différentes agences publiques et du secteur privé plutôt que de miser sur la création d'une base de données centrale (Kattel et Mergel, 2019).

6 « X-Road, qui est le fondement du gouvernement électronique estonien, est un logiciel open source et un écosystème qui fournit un échange de données unifié et sécurisé entre les organisations des secteurs privés et publics. Il permet aux divers systèmes d'information des services électroniques des secteurs public et privé du pays de se connecter et de fonctionner en harmonie. " (e-Estonia, trad., 2023).

Ultimement, et à la différence de l'identité numérique britannique, le dispositif estonien a pu jouir d'une certaine forme de succès dans la mesure où il fut en mesure de favoriser l'adoption de son SGING tant au niveau des organisations qu'en ce qui a trait à la population, notamment en impliquant le secteur privé. Il semble que le défi d'utilité perçue soit un des gages de succès du SGING estonien.

Australie

Depuis 2015, le gouvernement australien développe une identité numérique nationale en réponse aux coûts associés à un écosystème d'identité numérique fragmenté pour l'économie numérique australienne. De manière plus concrète, ce système lancé en 2019 se divise en deux parties, soit le Système d'identité numérique (*Digital Identity System*) ainsi que le Cadre d'identité numérique de confiance (*Trusted Digital Identity Framework*). Alors que c'est au sein du Système suivant le modèle fédéré que l'on retrouve l'offre de service, réservé aux agences fédérales pour l'instant, le Cadre représente une accréditation attestant que l'organisation (ex. fournisseur d'identité) respecte les standards établis par le gouvernement australien. Alors que le secteur privé (ex. Mastercard) peut recevoir une accréditation du Cadre, il ne peut pas fournir des services au sein du Système. Par ailleurs, l'administration du Système relève actuellement de l'autorité de contrôle intérimaire tandis que l'opération de ce dernier se fait par Services Australie (*Services Australia*).

Plusieurs défis se sont présentés lors de ce projet d'identité numérique. Premier défi: la faible adoption par la population de cette identité numérique. En date de 2020, 1,7 million d'Australiens avaient fait usage du système sur une population de près de 26 millions. Dans le même sens, la non-participation au Système des différents territoires, États et du secteur privé additionné à la gouvernance actuelle du système, réservé au gouvernement fédéral, ont constitué un autre défi à l'adoption de cette identité par la société australienne.

En réponse à ces défis, le gouvernement australien proposa en 2021 le *Trusted Digital Identity Bill* visant notamment la création d'une entité de contrôle permanente et d'un nouveau système parallèle permettant aux différentes entités privées, territoriales et étatiques d'offrir des services aux usagers par le biais de cette identité (Shah, 2022 et Australian Government, 2023). De plus, ce cadre propose de nouvelles mesures pour renforcer la protection de la vie privée.

Ultimement, le cas australien démontre le caractère interrelié des différents défis identifiés dans la mesure où, en voulant résoudre certains problèmes liés à la gestion et l'organisation (inclusion de davantage d'acteurs), le gouvernement a dû adopter des réformes pour résoudre les contraintes en lien avec les défis liés aux lois et normes. De plus, le modèle australien représente un SGING où le gouvernement occupe, à la différence du modèle estonien, davantage le rôle de régulateur que de fournisseur d'identités.

Suède

C'est au début des années 2000, tout comme l'Estonie, que la Suède entama le développement d'une identité numérique nationale. Dès le début de la conception de cette identité, le gouvernement suédois fit le choix de ne pas développer lui-même le SGIN mais préféra prendre la posture de régulateur et de certificateur plutôt que d'opérateur ou de développeur sur le dossier du SGIN. Le développement se fit surtout avec le secteur bancaire pour bénéficier de ses infrastructures, de sa clientèle, de sa crédibilité ainsi que la sécurité de ces dernières (Pöhn, Grabatin, et Hommel 2021). En ce sens, ce n'est pas le gouvernement qui agit à titre de fournisseur d'identités, mais bien le secteur privé (3 organisations). Autrement dit, on utilise ici un dispositif développé par le privé, majoritairement *BankID*, pour interagir avec le gouvernement plutôt que l'inverse comme désiré en Australie avec l'introduction du *Trusted Digital Identity Bill*.

Singapour

Lancé en 2003 par le gouvernement de Singapour, le système *Singpass* et *Corppass* permet tant aux organisations qu'aux individus de s'identifier auprès des organisations publiques et privées. Autrement dit, le gouvernement occupe dans ce système le rôle de fournisseur d'identités ainsi que le rôle de fournisseur de services tandis que les organisations non gouvernementales représentent des fournisseurs de services. À cet égard, la collaboration avec des acteurs provenant du secteur privé, dont le secteur financier, fut essentielle à l'adoption de cette identité nationale.

Depuis son lancement, cette identité numérique nationale, fondée sur le système d'identité nationale préexistant, subit plusieurs modifications, dont l'introduction de l'authentification à deux facteurs en 2014 ainsi que l'introduction d'un portefeuille numérique en 2022. D'un point de vue technique, *Singpass* et *Corppass* reposent sur la passerelle APEX qui vise à faciliter l'échange de données de manière sécuritaire ainsi que sur une infrastructure à clés publiques. Parallèlement, plusieurs lois furent créées, ayant pour objectif d'encadrer et de faciliter la transformation numérique du gouvernement singapourien.

Alors que *Singpass* jouit d'un succès auprès de la population (97% de la population éligible utilisent l'application en 2022), plusieurs raisons peuvent expliquer son succès. D'emblée, les multiples applications de cette identité numérique dans la vie de tous les jours, facilitées par l'implication du secteur privé, influencent positivement l'utilité perçue de cette identité numérique. De plus, la facilité d'utilisation perçue (ex. portefeuille numérique) et le contrôle dont disposent les individus sur leurs données contribuent au succès de ce SGING. Ultimement, le cas singapourien représente un exemple de succès (Banque mondiale, 2022).

Finlande

L'année 1999 marque le lancement de la carte d'identité numérique finlandaise (FINeID[7]), la première du genre au monde (Rissanen, 2010). Par ailleurs, c'est dans un contexte de remplacement de l'ancienne carte d'identité nationale qu'elle fut introduite. Autrement dit, cette nouvelle forme d'identité numérique, contenant notamment une adresse et un code d'identification unique (ex. numéro d'assurance sociale), se base sur la carte d'identité nationale non obligatoire. Parallèlement, les institutions financières finlandaises lancèrent leur propre identité numérique nommée TUPAS qui jouit d'un plus grand succès auprès de la population. En effet, en 2010, 99% des connexions aux services gouvernementaux en ligne se firent par le biais de TUPAS plutôt que par le biais de la carte d'identité nationale contenant une identité numérique. En 2003, le gouvernement finlandais permit l'utilisation de TUPAS pour accéder à ses services malgré le fait qu'elle fut jugée moins sécuritaire. Ultimement, la faible adoption du SGING développé par le gouvernement finlandais limita l'utilité perçue de ce dernier par la population. On note ici l'importance de l'effet de réseau[8] pour un SGING (Rissanen, 2010).

Dans un autre ordre d'idées, l'adoption du *Finish Trust Network*[9] (FTN) en 2017, gérée par l'agence gouvernementale Traficom, additionnée de l'adoption de lois renforçant les moyens d'authentifications mit fin à TUPAS en 2019. De manière plus concrète, le FTN, développé conjointement avec le secteur privé, a pour objectif de renforcer et simplifier l'identification en ligne. De plus, on retrouve dans le FTN une multitude de fournisseurs d'identités et d'intermédiaires faisant le lien entre les organisations ayant recours au FTN et les fournisseurs d'identités.

Le cas finlandais démontre l'importance de l'utilité perçue d'un SGING en ce qui a trait à son succès. En effet, le peu de cas d'utilisation offert par le SGING développé par le gouvernement finlandais par rapport à la solution du secteur privé explique en grande partie l'échec de celle-ci. En ce sens, cela ne signifie pas pour autant une déresponsabilisation de la part du gouvernement vu l'adoption du FTN en 2017. Au contraire, alors que le gouvernement finlandais occupait essentiellement un rôle de fournisseur d'identités, il occupe dorénavant davantage le rôle de régulateur. En ce sens, un échec relatif à un SGING ne représente pas pour autant une fatalité dans son déploiement à long terme. En effet, des ajustements sont possibles en cours de déploiement.

Danemark

Le gouvernement danois lança en 2002 le système OCES représentant une forme de signature électronique ainsi qu'un moyen de s'authentifier en ligne. Développé par le secteur privé, OCES ne jouit pas immédiatement d'un succès auprès de la population danoise en raison d'un manque de bénéfices perçus et de la présence de problèmes techniques. En 2010, le gouvernement danois, en partenariat avec le secteur financier, mit à la disposition de la population la seconde génération du SGING, soit NemID. Cette nouvelle identité, dont les cas d'utilisation ont été élargis, permette l'accès aux services des secteurs privés et publics, ce qui facilita son adoption par la population, d'autant plus que le gouvernement adopta une loi en 2015 rendant obligatoire l'utilisation des services en ligne. De plus, NemID, à l'origine sur une carte physique, fut bonifié par l'introduction d'une application mobile en 2018. En 2022, le gouvernement danois déploya la troisième génération du système maintenant nommé MitID en partenariat avec le secteur privé (FR1) fondé sur le modèle de fédération et d'autorisation par courtiers. Quoique similaire à NemId, MitID est jugé plus sécuritaire. (Agency for Digital Government 2023; Hoff et Hoff 2010)

7 Malgré sa faible popularité, FINeID existe toujours.

8 L'effet de réseau peut se résumer par la formule suivante : plus le nombre d'usagers d'un réseau augmente, plus sa valeur augmente aux yeux des usagers.

9 Le FTN représente l'écosystème répondant aux normes établies par *l'Act on Strong Electronic Identification and Electronic Signatures*.

Tableau 1 - Récapitulatif des SGING étudiés

États	Nom	Année d'introduction	Modèle	Implication du secteur privé	Taux d'adoption	Utilisation(s)	Obligatoire pour la population?	Rôle de l'État
Singapour	Singpass Corppass	2003	Fédéré	Fournisseur de services	97 % (2022)	Accès aux services du gouvernement et du secteur privé	Non	Régulation Fournisseur de services Fournisseur d'identité
Suède	BankID[10]	2003	Fédéré	Fournisseurs d'identités et de services Conception et développement Financement	99 % (2023)	Accès aux services du gouvernement et du secteur privé	Non	Régulation Fournisseur de services
Australie	Trusted Digital Identity Framework/ Digital Identity System	2019	Fédéré (MyGovID, DigitaliD, etc.)	N/A	N/A	Accès aux services du gouvernement	Non	Régulation Fournisseur de services Fournisseur d'identité
Estonie	e-Identity	2002	Fédéré	Fournisseurs de services Développement	98 % (2018)	Accès aux services du gouvernement et du secteur privé	Oui	Régulation Fournisseur de services Fournisseur d'identité
Royaume-Uni	GOV.UK Verify	2016-2022	Fédéré	Fournisseurs d'identités	5,4 millions (2020) (25 millions prévu en 2020)	Accès aux services du gouvernement	Non	Régulation Fournisseur de services
Finlande	Finnish Trust Network	2017	Fédéré (FINeID, BankID, etc.)	N/A	N/A	Accès aux services du gouvernement et du secteur privé	Non	Régulation Fournisseur de services
Danemark	MitID	2002	Fédéré	Fournisseurs d'identités et de services Conception et développement 97 % (2022)	90 % (2023)	Accès aux services du gouvernement et du secteur privé	Non	Régulation Fournisseur de services Fournisseur d'identité

10 Malgré l'existence de plusieurs identités numériques, BankID jouit d'un quasi-monopole.

CONCLUSIONS ET PISTES D'ACTION

À la lumière de notre revue de la littérature et de nos études de cas, **il ressort que l'utilité perçue d'une identité numérique nationale est essentielle à son succès, ce qui peut se traduire par son adoption par la population.** Cette utilité est déterminée par la possibilité d'utiliser cette dernière au quotidien. Pour ce faire, il importe d'une part d'impliquer les différents acteurs gouvernementaux ainsi que ceux issus du secteur privé (ex. institutions financières) afin qu'ils intègrent cette identité nationale numérique. D'autre part, il est important de consulter la population, utilisatrice de cette identité, afin de développer un système répondant aux besoins de celle-ci. Finalement, le type de modèle de SGING sélectionné n'apparaît pas comme un gage de succès au regard des exemples présentés.

Il est également important d'accompagner le développement des SGING par l'adoption ou la modification de normes et de lois et par la mise en place d'une entité supervisant le SGING. De plus, la présence d'une autorité centrale assurant une gouvernance verticale permet de faciliter la coordination entre les différents acteurs impliqués. Il importe aussi de mettre à la disposition des acteurs impliqués les ressources techniques, humaines et financières pour assurer le développement et le maintien du SGING.

Pour conclure, nous proposons ici quelques pistes d'action

1. Il importe d'adopter des cadres réglementaires avant le déploiement des SGING dans le but d'encadrer ces systèmes d'identification, voire de les rendre possibles, notamment en ce qui a trait à l'utilisation et la protection des données personnelles.
2. La présence d'une autorité de coordination centrale est essentielle pour assurer la communication entre les différents acteurs impliqués, pour définir leurs rôles ainsi que pour la définition d'une stratégie.
3. Il importe d'impliquer les acteurs concernés ou pouvant être touchés (population, secteur privé, différentes agences gouvernementales, etc.) dans le but de développer un SGING convenant au plus grand nombre d'acteurs.
4. Le SGING doit bénéficier des ressources financières, techniques et humaines adéquates. Dans un autre ordre d'idées, le déploiement de celui-ci bénéficierait de se faire par cas d'utilisation avec complexité croissante.
5. Plus les opportunités d'usage d'un SGING sont élevées, plus l'adoption risque d'être grande. En ce sens, il convient d'adopter une approche centrée sur l'utilisateur.
6. Il importe de favoriser la protection de la vie privée et le contrôle des utilisateurs sur leurs données personnelles.
7. Une gouvernance verticale serait davantage appropriée à la réalité des SGIN qu'une gouvernance de type horizontal.

ANNEXES

Figure 5 - Exemples de SGIN gouvernementaux (Banque mondiale, 2016, 25)

RÉFÉRENCES

Abraham, Sunil. 2020. « Building Trust: Lessons from Canada's Approach to Digital Identity ». *ORF Issue Brief*, no 367.

Agency for Digital Government. 2023. « MitID – a Unique Public-Private Partnership ». 2023. https://en.digst.dk/systems/mitid/mitid-a-unique-public-private-partnership/.

Alkhalifah, Ali. 2013. « Factors Affecting User Adoption of Identity Management Systems: An Empirical Study ». Sydney: University of New South Wales. http://unsworks.unsw.edu.au/fapi/datastream/unsworks:11554/SOURCE01?view=true.

Al-Nidawi, Wael Jabbar Abed, Mahdi Athab Maan, et Marini Othman. 2015. « Review on National Electronic Identification System ». In *2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, 228-33. https://doi.org/10.1109/ACSAT.2015.42.

Arora, Siddhartha. 2008. « National e-ID card schemes: A European overview ». *Information Security Technical Report* 13 (2): 46-53. https://doi.org/10.1016/j.istr.2008.08.002.

Avellaneda, Oscar, Alan Bachmann, Abbie Barbir, Joni Brenan, Pamela Dingle, Kim Hamilton Duffy, Eve Maler, Drummond Reed, et Manu Sporny. 2019. « Decentralized Identity: Where Did It Come From and Where Is It Going? » *IEEE Communications Standards Magazine* 3 (4): 10-13. https://doi.org/10.1109/MCOMSTD.2019.9031542.

Banque mondiale. 2022. « National Digital Identity and Government Data Sharing in Singapore: A Case Study of Singpass and APEX ». Banque mondiale. https://doi.org/10.1596/38201.

_____. 2016. « Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation ». Banque mondiale. https://documents1.worldbank.org/curated/en/600821469220400272/pdf/107201-WP-PUBLIC-WB-GSMA-SIADigitalIdentity-WEB.pdf.

Bernat, Laurent. 2011. « National Strategies and Policies for Digital Identity Management in OECD Countries .» *OECD Digital Economy Papers*. Paris, France: Organisation for Economic Cooperation and Development (OECD). https://www.proquest.com/docview/863240193/abstract/885909AF6F14648PQ/6.

Committee of Public Accounts. 2019. « Accessing Public Services through the Government's Verify Digital System .» House of Commons. https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/1748/1748.pdf

Dixon, Pam. 2017. « A Failure to "Do No Harm" -- India's Aadhaar Biometric ID Program and Its Inability to Protect Privacy in Relation to Measures in Europe and the U.S. » *Health and Technology* 7 (4): 539-67. https://doi.org/10.1007/s12553-017-0202-6.

Eaton, Ben, Jonas Hedman, et Rony Medaglia. 2018. « Three Different Ways to Skin a Cat: Financialization in the Emergence of National e-ID Solutions ». *Journal of Information Technology* 33 (1): 70-83. https://doi.org/10.1057/s41265-017-0036-8.

Eke, Damian, Ridwan Oloyede, Paschal Ochang, Favour Borokini, Mercy Adeyeye, Lebura Sorbarikor, Bamidele Wale-Oshinowo, et Simisola Akintoye. 2022. « Nigeria's Digital Identification (ID) Management Program: Ethical, Legal and Socio-Cultural Concerns ». *Journal of Responsible Technology* 11 (octobre): 100039. https://doi.org/10.1016/j.jrt.2022.100039.

e-Estonia. 2023. « E-Estonia .» E-Estonia. 15 février 2023. https://e-estonia.com/.

Fathiyana, Rana, Fadhil Hidayat, et Budi Rahardjo. 2020. « An Integration of National Identity towards Single Identity Number with Blockchain .» In *Proceedings of the 7th Mathematics, Science, and Computer Science Education International Seminar*.

Fioravanti, Fabio, et Enrico Nardelli. 2008. « Identity Management for E-Government Services ». In *Digital Government: E-Government Research, Case Studies, and Implementation*, édité par Hsinchun Chen, Lawrence Brandt, Valerie Gregg, Roland Traunmüller, Sharon Dawes, Eduard Hovy, Ann Macintosh, et Catherine A. Larson, 331-52. Integrated Series In Information Systems. Boston, MA: Springer US. https://doi.org/10.1007/978-0-387-71611-4_17.

Gariépy, Félix. 2023. « L'acceptabilité sociale de l'identité numérique chez les organisations québécoises : le cas du Service québécois d'identité numérique ». Sherbrooke: Université de Sherbrooke. Mémoire de maîtrise.

Geteloma, V., C. K. Ayo, et R. N. Goddy-Wurlu. 2019. « A Proposed Unified Digital Id Framework for Access to Electronic Government Services ». *Journal of Physics: Conference Series* 1378 (4). https://doi.org/10.1088/1742-6596/1378/4/042039.

Gil-García, J. Ramón, et Theresa A. Pardo. 2005. « E-Government Success Factors: Mapping Practical Tools to Theoretical Foundations ». *Government Information Quarterly* 22 (2): 187-216. https://doi.org/10.1016/j.giq.2005.02.001.

Gouvernement du Canada. 2016. « Guideline on Identity Assurance ». Guideline on Identity Assurance. 2016. https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=30678&section=html.

Grönlund, Åke. 2010. « Electronic Identity Management in Sweden: Governance of a Market Approach .» *Identity in the Information Society* 3 (1): 195-211. https://doi.org/10.1007/s12394-010-0043-1.

Hilowle, Malyun Muhudin, William Yeoh, Marthie Grobler, Graeme Pye, et Frank Jiang. 2023. « Towards Improving the Adoption and Usage of National Digital Identity Systems ». In *Proceedings of the 37th IEEE/ACM International Conference on Automated Software Engineering*, 1-6. ASE '22. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3551349.3561144.

Hilowle, Malyun, William Yeoh, Marthie Grobler, Graeme Pye, et Frank Jiang. 2022. « Users' Adoption of National Digital Identity Systems: Human-Centric Cybersecurity Review ». *Journal of Computer Information Systems* 0 (0): 1-16. https://doi.org/10.1080/08874417.2022.2140089.

Hoff, Jens Villiam, et Frederik Villiam Hoff. 2010. « The Danish EID Case: Twenty Years of Delay ». *Identity in the Information Society* 3 (1): 155-74. https://doi.org/10.1007/s12394-010-0056-9.

Kattel, Rainer, et Ines Mergel. 2019. « Estonia's Digital Transformation: Mission Mystique and the Hiding Hand ». In *Great Policy Successes*, édité par Paul 't Hart et Mallory Compton, 0. Oxford University Press. https://doi.org/10.1093/oso/9780198843719.003.0008.

Krishna, Shyam. 2021. « Digital Identity, Datafication and Social Justice: Understanding Aadhaar Use among Informal Workers in South India .» *Information Technology for Development* 27 (1): 67-90. https://doi.org/10.1080/02681102.2020.1818544.

Kubicek, Herbert. 2010. « Introduction: Conceptual Framework and Research Design for a Comparative Analysis of National EID Management Systems in Selected European Countries .» *Identity in the Information Society* 3 (1): 5-26. https://doi.org/10.1007/s12394-010-0052-0.

Kubicek, Herbert, et Torsten Noack. 2010. « Different Countries-Different Paths Extended Comparison of the Introduction of EIDs in Eight European Countries .» *Identity in the Information Society* 3 (1): 235-45. https://doi.org/10.1007/s12394-010-0063-x.

Lentner, Gabriel M., et Peter Parycek. 2016. « Electronic Identity (EID) and Electronic Signature (ESig) for EGovernment Services - a Comparative Legal Study ». *Transforming Government: People, Process and Policy* 10 (1): 8-25. https://doi.org/10.1108/TG-11-2013-0047.

Lips, Miriam. 2010. « Rethinking Citizen - Government Relationships in the Age of Digital Identity: Insights from Research .» *Information Polity* 15 (4): 273. https://www.proquest.com/docview/853271100/1F0AB308DA884FEFPQ/11.

Mahula, Stanislav, Evrim Tan, et Joep Crompvoets. 2021. « With blockchain or not? Opportunities and challenges of self-sovereign identity implementation in public administration: Lessons from the Belgian case ». In *DG. O2021: The 22nd Annual International Conference on Digital Government Research*, 495-504.

Mariën, Ilse, et Leo Van Audenhove. 2010. « The Belgian E-ID and Its Complex Path to Implementation and Innovational Change ». *Identity in the Information Society* 3 (1): 27-41. https://doi.org/10.1007/s12394-010-0042-2.

Martens, Tarvi. 2010. « Electronic Identity Management in Estonia between Market and State Governance .» *Identity in the Information Society* 3 (1): 213-33. https://doi.org/10.1007/s12394-010-0044-0.

Medaglia, Rony, Jonas Hedman, et Ben Eaton. 2017. « Public-Private Collaboration in the Emergence of a National Electronic Identification Policy ». In *Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS*.

Melin, Ulf, Karin Axelsson, et Fredrik Söderström. 2013. « Managing the development of secure identification-investigating a national e-ID initiative within a public e-service context ». In *21st European Conference on Information Systems, June 5-8, 2013, Utrecht, The Netherlands*.

_____. 2016. « Managing the Development of E-ID in a Public e-Service Context .» *Transforming Government: People, Process and Policy* 10 (1): 72-98. https://doi.org/10.1108/TG-11-2013-0046.

Mettler, Tobias, et Ali A. Guenduez. 2019. « From SuisseID to SwissID: Overcoming the key challenges in Switzerland's e-credential market ». In *Fortieth International Conference on Information Systems*.

Ngwenyama, Ojelanki, Helle Zinner Henriksen, et Daniel Hardt. 2021. « Public management challenges in the digital risk society: A critical analysis of the public debate on implementation of the Danish NemID ». *European Journal of Information Systems*, 1-19.

OECD. 2011. « National Strategies and Policies for Digital Identity Management in OECD Countries .» IDEAS Working Paper Series from RePEc. St. Louis, United States: Federal Reserve Bank of St. Louis. 2011. https://www.proquest.com/docview/1698938810/2B62A06968DE4BA5PQ/32.

OCDE. 2011. « National Strategies and Policies for Digital Identity Management in OECD Countries ». Paris: OCDE https://doi.org/10.1787/5kgdzvn5rfs2-en.

Okunoye, Babatunde, et this link will open in a new window Link to external sites. 2022. « Mistrust of Government within Authoritarian States Hindering User Acceptance and Adoption of Digital IDs in Africa: The Nigerian Context .» *Data & Policy* 4. https://doi.org/10.1017/dap.2022.29.

Panigrahi, Subhashish. 2022. « MarginalizedAadhaar: India's Aadhaar Biometric ID and Mass Surveillance .» *Interactions* 29 (2): 16. https://doi.org/10.1145/3517173.

Pöhn, Daniela, Michael Grabatin, et Wolfgang Hommel. 2021. « EID and Self-Sovereign Identity Usage: An Overview ». *Electronics* 10 (22): 2811. https://doi.org/10.3390/electronics10222811.

Ribeiro, Carlos, Herbert Leitold, Simon Esposito, et David Mitzam. 2018. « STORK: A Real, Heterogeneous, Large-Scale EID Management System ». *International Journal of Information Security* 17 (5): 569-85. https://doi.org/10.1007/s10207-017-0385-x.

Rissanen, Teemu. 2010. « Electronic Identity in Finland: ID Cards vs. Bank IDs .» *Identity in the Information Society* 3 (1): 175-94. https://doi.org/10.1007/s12394-010-0049-8.

Shah, Rajiv. 2022. « The Future of Digital Identity in Australia .» Australia Strategic Policy Institute. https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2022-11/The%20future%20of%20digital%20identity%20in%20Australia.pdf?VersionId=EFEVDX3F3uEtC4IX98n39JpQoEJjxx2S.

Uesugi, Shiro, Masashi Ueda, et Yoshikazu Ujikane. 2011. « An Identification Management Framework for IT-Enabled Services and E-Government: A Consideration of the Case of Japan ». *Applied Mechanics and Materials* 135-136 (octobre): 222. https://doi.org/10.4028/www.scientific.net/AMM.135-136.222.

Union internationale des télécommunications. 201apr. J.-C. « Digital Identity Roadmap Guide ». Union internationale des télécommunications. https://www.itu.int/en/ITU-D/ICT-Applications/Documents/Guides/ITU_eID4D_DIGITAL%20IDENTITY_ROAD_MAP_GUIDE_FINAL_Under%20Review_Until-05-10-2018.pdf.

Vérificateur général du Québec. 2012. « Rapport du Vérificateur général du Québec à l'Assemblée nationale pour l'année 2012-2013 - Contrats de service professionnels liés au traitement de l'information ». Vérificateur général du Québec. https://www.vgq.qc.ca/Fichiers/Publications/rapport-annuel/2012-2013-VOR-Automne/fr_Rapport2012-2013-VOR-Automne-Chap05.pdf.

obvia

www.obvia.ca