

**QUE
RECHERCHER
DANS LES
SYSTÈMES
D'IDENTITÉ
NUMÉRIQUE**

**une typologie
des étapes à
suivre**

Ce rapport est basé sur des recherches menées par The Engine Room, avec le soutien d'Omidyar Network, d'Open Society Foundations et de la Fondation Yoti, d'octobre 2018 à octobre 2019.

Recherche: Sharid Bin Sha que, Chenai Chair, Kittima Leeruttanawisut, Koliwe Majama, Chuthathip Maneepong, Precious Ogbuji, Berhan Taye

Auteur: Sara Baker, The Engine Room

Révision et corrections : Zara Rahman, Laura Guzmán, Madeleine Maxwell, Sivu Siwisa, The Engine Room

Traduction: Global Voices

Mise en page et illustrations : Julie Saw, Little by Little Studio

Le texte de ce rapport est publié sous une licence Creative Commons Partage dans les Mêmes Conditions 4.0 International. Pour voir une copie de cette licence, visitez le site <http://creativecommons.org/licenses/by-sa/4.0/>.

THE ENGINE ROOM

Contexte du projet

Fin 2018, The Engine Room a commencé un projet visant à comprendre les expériences des personnes avec les systèmes d'identité numérique. Pour les besoins de ce projet, nous avons défini les systèmes d'identité numérique comme étant des systèmes étatiques ou humanitaires qui collectent et utilisent des données numériques, comprenant souvent des données biométriques telles que des empreintes digitales et des scans d'iris, afin d'identifier les citoyens, les résidents et les bénéficiaires.

Nous avons travaillé avec des chercheurs locaux dans cinq pays, en nous concentrant sur les systèmes nationaux au Nigeria, au Zimbabwe et en Thaïlande, ainsi que sur les systèmes humanitaires installés dans les camps de réfugiés Rohingya au Bangladesh et en Éthiopie. Pour mieux comprendre l'écosystème d'identité numérique au sens large, le projet comprenait une revue de la littérature allant bien au-delà des cinq sites susmentionnés, pour explorer des systèmes dans d'autres parties du monde.

Cette typologie des étapes à suivre constitue le premier résultat de nos recherches. D'autres réflexions, notamment un rapport global et des études de cas, sont à venir.

Comment utiliser cette typologie

Cette typologie décrit les étapes de la planification, du développement, de la mise en œuvre et de la maintenance des systèmes d'identité numérique, telles que définies par nos études sur le terrain et nos recherches documentaires. Elle est destinée à la société civile, aux militants et aux journalistes qui souhaitent développer leur compréhension de ces systèmes, éduquer ou faire du plaidoyer sur ceux-ci¹.

Cet outil vous aidera à :

- Identifier à quel stade se trouve un système d'identification numérique
- Comprendre ce qu'il faut attendre de chaque étape
- Développer des stratégies de plaidoyer pour influencer les développeurs et les décideurs

Chaque étape répertorie les activités clés pouvant être entreprises par les créateurs de systèmes, mais tous les systèmes que nous avons examinés n'incluaient pas toutes les activités.

Chaque activité est suivie d'une **liste de questions** à poser sur le système d'identification numérique de votre communauté, et chaque étape comprend une brève **étude de cas** sur le plaidoyer.

Les étapes de planification et de développement répertorient également les **documents clés** à examiner. Il s'agit de documents généralement produits par les développeurs de système d'identité numérique, qui permettent de mieux comprendre leurs motivations, leurs projets et leurs objectifs.

Vous trouverez plus d'informations sur certains des sujets mentionnés dans les références à la fin du document.

Étape 1 Planification

Dans cette étape, les créateurs du système d'identité établissent des bases en soulignant les problèmes que le système est censé résoudre et en créant des cadres nécessaires. Les questions clés à poser visent à approfondir les arguments avancés en faveur d'un système d'identité numérique et à mieux comprendre les fondements juridiques et politiques qui pourraient l'appuyer.

Développement de stratégie: Identifier le besoin d'identification numérique

Questions à poser

- Quel problème ce système d'identification numérique vise-t-il à résoudre? Est-ce un problème réel et important? Existe-t-il des preuves démontrant que l'identification numérique résoudra le problème?
 - Les arguments courants des États incluent :
 - › Le renforcement de la sécurité nationale
 - › L'amélioration du service et la distribution des droits
 - › L'inclusion financière
 - Les arguments courants des organisations humanitaires² incluent:
 - › Une distribution plus rapide et plus efficace de l'aide
 - › Une diminution de la fraude
- Qui profite le plus de ce système ? Les avantages l'emportent-ils sur les risques ?
- Le développeur a-t-il mené de sérieuses consultations avec divers acteurs?

Élaboration de politiques et législation: création des cadres réglementaires pour la mise en œuvre de l'identification numérique

Documents clés

- Législation sur la protection des données
- Projet de Loi sur l'identification numérique (ou une autre loi exigeant l'existence d'un système national)

Questions à poser

- Quelles lois existantes permettent ou empêchent la collecte de données, telles que des données biométriques, par le biais de ce système ?
- Quels projets de loi connexes les législateurs envisagent-ils? Ces projets de loi incluent-ils une période de consultation publique ?
- Existe-t-il des lois sur la protection des données déjà en place³ ? Comment, le cas échéant, affecteront-ils le système d'identification numérique prévu ? Traitent-ils des problèmes tels que le partage et la conservation des données ?

Étude de cas

Le recours juridique peut être un moyen efficace de lutte contre les atteintes à la vie privée et d'autres problèmes. Lorsque le secrétaire général du Parti National du Peuple a intenté une action en justice alléguant que le système d'identité numérique proposé par la Jamaïque était inconstitutionnel, la Cour Suprême de la Jamaïque s'est



prononcée⁴ en sa faveur et le système a été supprimé. Bien que des poursuites analogues en Inde n'ont pas permis de stopper leur propre système (Aadhaar) avant l'affaire de la Jamaïque, les efforts de l'Inde ont eu un impact important sur la Jamaïque, où les juges se sont largement appuyés sur l'opinion dissidente du juge de la Cour Suprême Indienne, DY Chandrachud.⁵

Étape 2 Développement

À cette étape, les développeurs travaillent avec des partenaires pour définir les paramètres et l'infrastructure du système d'identification numérique. Les principales questions à se poser portent sur la nature de ces partenariats et la protection des données des utilisateurs.

Marchés publics: recherche et passation de marchés avec un partenaire du secteur privé pour développer, et éventuellement maintenir un système d'identification numérique

Documents clés

- Appel à propositions et / ou termes de référence pour un tiers contractant
- Un accord de partage de données entre les gouvernements hôtes et les organisations d'aide humanitaire

Questions à poser

- Existe-t-il un processus d'achat ouvert et transparent ?⁶
- Qui est le fournisseur commercial et quels sont ses avantages ?
- À quelles données le fournisseur commercial a-t-il accès et que va-t-il en faire ?
- Le fournisseur commercial a-t-il des liens avec les services de renseignement nationaux et internationaux, et les forces de l'ordre ?
- Si une organisation telle que le HCR met en place un système au nom d'un gouvernement hôte, les données sont-elles partagées avec les pays d'origine des réfugiés ?

Conception et planification: création de l'architecture et des protocoles associés d'un système d'identification numérique

Documents clés

- Diagramme d'architecture ou autre tableau décrivant le fonctionnement du système
- Processus régissant le consentement, l'enregistrement, la conservation des données, etc.
- Évaluation des risques ou évaluation de l'impact sur la vie privée

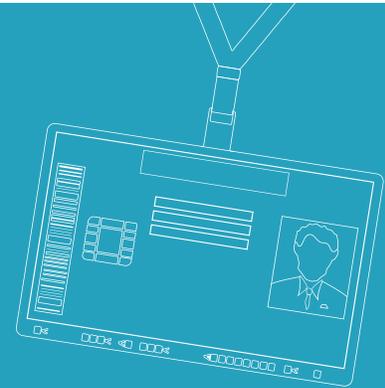
Questions à poser

- La conception de l'architecture du système suit-elle les pratiques de plus en plus recommandées telles que : Respect de la vie privée dès la conception⁷ , Conception centrée sur l'être humain⁸ , Conception participative⁹ ?
- Les processus d'enregistrement et de consentement sont-ils conçus avec la participation de groupes vulnérables ?
- Quels documents d'identité seront utilisés pour le processus d'inscription ? Est-ce que tout le monde possède déjà ces documents ? Qui pourrait être laissé de côté ?
- Où les données seront-elles stockées ? La base de données est-elle centralisée ? Qui y aura accès ?
- Existe-t-il des politiques et des protocoles de sécurité appropriés basés sur des évaluations de risque ?
- Existe-t-il des politiques de conservation des données ?

Étude de cas

Lorsque la Tunisie a proposé une carte d'identité biométrique, il n'y avait aucune information sur l'endroit où les données personnelles seraient stockées ou qui y aurait accès, et le fournisseur commercial n'a jamais été nommé¹⁰. La société civile a convaincu les législateurs d'adopter des amendements visant à protéger

la base de données biométriques¹¹. Dans une victoire éclatante, une fois les amendements adoptés, le Ministère de l'Intérieur a totalement abandonné le projet de loi. Il semble que celui-ci ne pouvait pas aller de l'avant sans donner à l'entreprise non nommée un accès aux données des citoyens.



Étape 3 Mise en oeuvre

Cette étape implique le déploiement et la mise en fonction du système d'identité numérique. Les questions clés à poser soulignent l'importance de la sensibilisation du public et cherchent à comprendre les expériences des personnes avec le système.

Campagnes de sensibilisation: informer la population sur le but, la fonction et le processus d'enregistrement d'un système d'identification numérique

Questions à poser

- Comment les développeurs ont-ils impliqué le public ?
 - Les tactiques courantes comprennent :
 - › Sensibilisation des médias
 - › Implication des leaders des communautés
 - › Annonces dans les camps de réfugiés
- Y a-t-il eu des contacts avec les groupes vulnérables ?
- Le public dispose-t-il d'informations suffisantes pour soutenir et utiliser les systèmes d'identification numérique ou plaider efficacement en faveur des changements critiques ?
- Les personnes peuvent-elles associer la confidentialité des données à d'autres problématiques urgentes telles que la pauvreté et la discrimination ?

Enregistrement et utilisation: inscription des utilisateurs dans un système d'identification numérique et activation des services

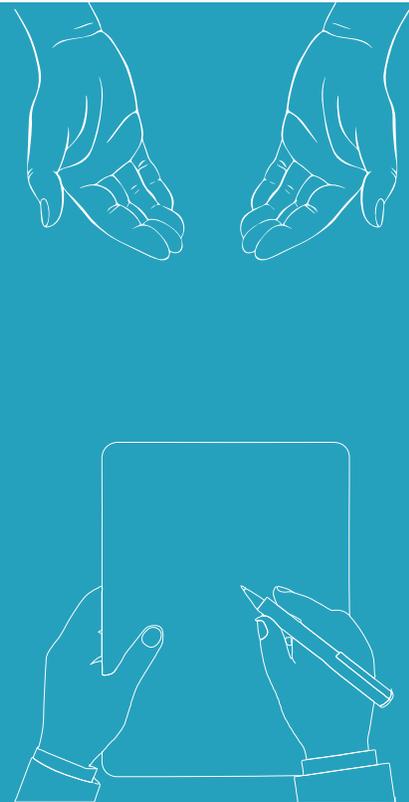
Questions à poser

- Les communautés marginalisées ont-elles été consultées afin d'éviter tout obstacle à l'enregistrement ?
 - Les obstacles communs incluent :
 - › Manque de lieux d'enregistrement accessibles pour les personnes handicapées et les personnes en zones rurales
 - › Discrimination à l'encontre des personnes transgenres et non binaires (par exemple, manque d'options appropriées en matière de genre sur les formulaires, incapacité à reconnaître les transitions de genre)

- › Manque d’alphabétisation dans les langues ou les outils numériques utilisés
 - › Incapacité à reconnaître les normes culturelles (par exemple, obliger les femmes des communautés conservatrices à s’inscrire indépendamment)
 - › Coûts liés à l’obtention ou à la fixation de documents d’identité initiaux
-
- Les organisations humanitaires ont-elles pris en compte l’impact des traumatismes sur les réfugiés nouvellement enregistrés ?
 - Toutes les populations bénéficient-elles des mêmes avantages? Y en-a-t-il qui subissent plus de préjudices que d’autres ?

Étude de cas

En Thaïlande, la société civile guide les migrants dans les étapes d’enregistrement des cartes d’identité. Ces liens étroits aussi bien avec les travailleurs migrants qu’avec les administrations qui établissent les cartes d’identité des migrants offrent une occasion précieuse de faire du plaidoyer. Les organisations de la société civile ont une connaissance unique des besoins des migrants ainsi que des obstacles et des risques auxquels ils sont confrontés, ce qui peut leur permettre de faire pression pour des changements qui profitent à cette population marginalisée.



Étape 4 Maintenance

Au cours de cette étape, les entités chargées d'exécuter un système d'identification numérique gèrent l'utilisation courante et les problèmes connexes. Bien que l'enregistrement attire généralement le plus d'attention, la maintenance est essentielle au succès à long terme d'un système d'identification numérique. Les questions à poser portent sur la manière dont les problèmes rencontrés par le système sont résolus et sur le sérieux avec lequel ces entités abordent le lourd fardeau de la sécurité.

Mise à jour : Traiter les changements de vie et les erreurs d'enregistrement dans un système d'identification numérique

Questions à poser

- Quel est le processus de mise à jour ou de correction des erreurs dans les données?
- Existe-t-il des preuves de l'efficacité ou de l'échec de ce processus ? Par exemple, des personnes ont-elles été dans l'incapacité de faire les changements nécessaires et cela a-t-il provoqué le déni d'un service, d'une aide ou de la capacité à exercer leurs droits ?
- Comment les faux positifs et les faux négatifs sont-ils gérés?¹²

Signalement de griefs: Soumission et traitement de plaintes concernant un système d'identification numérique

Questions à poser

- Comment les gens peuvent-ils porter plainte contre le système? Le processus est-il facile, intuitif et accessible ?
- Les personnes sont-elles traitées équitablement et avec respect lors du signalement des griefs ?
- Les gens font-ils confiance aux services chargés de répondre aux griefs ?
- Une surveillance indépendante est-elle nécessaire ?

Sécurité : Protéger un système d'identification numérique au fil du temps

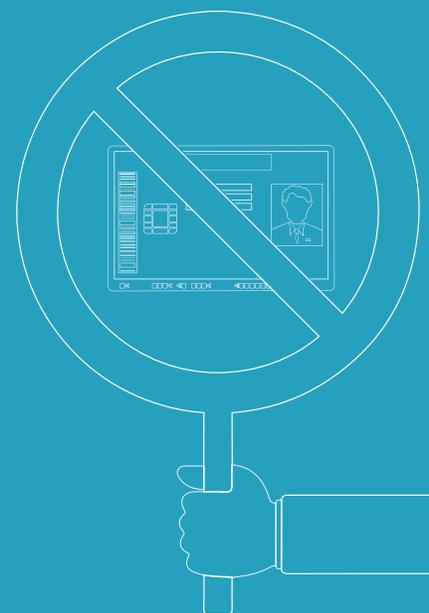
Questions à poser

- Le développeur respecte-t-il les politiques et les protocoles conçus pour éviter les incidents de sécurité ?
- Existe-t-il des protocoles clairs et viables pour traiter les fuites, les violations et les défaillances de données ?
- Le développeur est-il transparent sur le volume et les préjudices causés par les incidents de sécurité ?
- Existe-t-il des moyens pour que les personnes recherchent réparation des dommages résultant d'incidents de sécurité ?

Étude de cas

Lorsque les plaintes ne sont pas traitées, l'action collective peut avoir un impact. Au Bangladesh, avec peu de moyens à leur disposition pour affirmer leur pouvoir, les réfugiés Rohingya ont organisé une grève pour protester

contre les cartes intelligentes qui identifiaient chaque personne comme étant un «ressortissant du Myanmar déplacé de force», plutôt que comme un Rohingya, et pour exiger que les autorités refusent de partager des données biométriques sur les réfugiés avec le gouvernement du Myanmar.¹³



Notes

- 1** Pour les meilleures pratiques d'identification numérique, voir le mouvement «Good ID» (<https://www.good-id.org/en/>), le Cadre d'évaluation du Center for Internet and Society (<https://digitalid.design/evaluation-framework-01.html>), la feuille de route de l'UIT (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) et les principes de la Banque Mondiale (<http://documents.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf>).
- 2** The Engine Room et Oxfam. (2018). Les données Biométriques dans le Secteur Humanitaire <https://www.theengineroom.org/wp-content/uploads/2018/05/Oxfam-Report-May2018.pdf>
- 3** L'article de KJ Dearie sur la transparence, la responsabilité et le contrôle des utilisateurs dans les lois de protection de la vie privée. <https://www.good-id.org/en/articles/new-age-data-privacy-3-core-concepts-privacy-laws-around-world/>
- 4** Robinson v. le Procureur Général de la Jamaïque, JMFC Full 04 (Supreme Court, 2019). <https://supremecourt.gov.jm/sites/default/files/judgments/Robinson%2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf>
- 5** Bhatia, G. (2019, April 15). La vie d'après la dissidence d'Aadhaar: la Cour Suprême de la Jamaïque annule une identification biométrique nationale. Medianama. <https://www.medianama.com/2019/04/223-the-afterlife-of-the-aadhaar-dissent-the-jamaican-supreme-court-strikes-down-a-national-biometric-identification-gautam-bhatia/>
- 6** En savoir plus sur les contrats ouverts et les marchés publics <https://standard.open-contracting.org/infrastructure/latest/en/>
- 7** En savoir plus sur le respect de la vie privée dès la conception <https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/>

8 Pour en savoir plus sur la conception centrée sur l'humain, voir <https://www.ideo.org/tools>

9 Sinni, G. (2017). Conception participative pour les services publics: L'innovation dans l'administration publique. The Design Journal, 20(1), S3368-S3379, <https://doi.org/10.1080/14606925.2017.1352841>

10 Mzalouat, P.H. (2018, March 22). Carte d'identité biométrique : Chronique d'un projet de loi avorté. Inkyfada. <https://inkyfada.com/fr/2018/03/22/carte-identite-biometrique-tunisie/>

11 Sayadi, E. (2018, January 11). Carte d'identité biométrique c/ vie privée: Les Tunisiens ont gagné sur la vie privée! Mais ce n'est pas encore fini. <https://www.accessnow.org/biometric-id-vs-privacy-tunisians-stood-privacy-not-yet/>

12 Faux positif: lorsque le système identifie une correspondance où il ne devrait pas. Faux négatif: lorsque le système ne parvient pas à identifier une correspondance où il le devrait.

13 Islam, M. N. (26 novembre 2018). Le Bangladesh fait face à la colère des réfugiés à propos du terme 'Rohingya' et de la collecte de données. Reuters. <https://www.reuters.com/article/us-myanmar-rohingya-bangladesh/bangladesh-faces-refugee-anger-over-term-rohingya-data-collection-idUSKCN1NV1EN>