Unlocking Public and Private Finance for the Poor

Le rôle des transactions électroniques et des systèmes nationaux d'identification numérique dans l'économie numérique

BRIEF

Dans le cadre de la numérisation des économies, un programme d'identification numérique efficace démocratise l'accès aux transactions électroniques et aux services offerts par voie numérique, tels que l'éducation, les soins de santé et les services financiers. L'absence d'un système d'identification numérique universel accentue l'exclusion dans une économie numérique.

Ce note, rédigé en étroite collaboration avec Macmillan Keck, cherche à identifier les caractéristiques spécifiques des transactions électroniques et des cadres nationaux d'identification numérique qui peuvent aider les décideurs et les régulateurs à construire une économie numérique qui inclut - et sert - tout le monde.

Mars 2022

Macmillan Keck

Seharish Gillani, Ahmed Dermish, and Jeremiah Grossman of the UNCDF Policy Accelerator

Considérations à la lecture de cette note

1. Quels défis liés aux systèmes d'identification numérique et aux transactions électroniques dans l'économie numérique sont les plus importants sur votre marché, à la fois a) en général et b) pour les groupes mal desservis tels que les femmes et les personnes à faible revenu ?

2. Les systèmes d'identification numérique et les réglementations relatives aux transactions électroniques dans votre pays sont-ils concernés ?
   - **La numérisation** : L'application du système d'identification numérique et de la réglementation des transactions électroniques à l'économie numérique ?
   - **L'Inclusivité** : Les défis spécifiques du système d'identification numérique et des transactions électroniques auxquels sont confrontés les femmes, les personnes à faible revenu et/ou d'autres groupes mal desservis ?

3. Quelles entités sont responsables de la réglementation des systèmes d'identification numérique et des transactions électroniques ? Les responsabilités sont-elles claires, et des mécanismes sont-ils en place pour éviter l'arbitrage réglementaire ? Si ce n'est pas le cas, comment cela pourrait-il être amélioré ?

Résumé

Pour soutenir l'économie numérique, les cadres de transactions électroniques traduisent les concepts juridiques conventionnels qui sont essentiels à la conduite du commerce en équivalents numériques. Cela inclut la reconnaissance de l'effet juridique des signatures électroniques dans les transactions commerciales à la place des équivalents traditionnels sur papier. Les signatures numériques sont un sous-ensemble des signatures électroniques qui utilisent la cryptographie de l'infrastructure à clé publique et les certificats numériques pour fournir une sécurité et une fiabilité supplémentaires.

Les systèmes d'identification numérique stockent et capturent électroniquement l'identité numérique d'un individu, ce qui permet de les utiliser pour soutenir des services numériques ou des transactions électroniques. Les systèmes nationaux d'identification numérique sont des systèmes fondamentaux mis en œuvre par le gouvernement, ou sous ses auspices et accessibles à l'ensemble de la population. Les organisations internationales ont développé de bonnes pratiques et des garanties pour la conception et la mise en œuvre des systèmes nationaux d'identification numérique, notamment pour s'assurer qu'un système est inclusif et soutenu par des cadres appropriés de protection des données, de cybersécurité et de sécurité des données.

Les personnes s'inscrivent généralement auprès de ces systèmes en fournissant des données biographiques et, de plus en plus, biométriques. Les systèmes valident ensuite les données et dédupliquent l'identité de l'individu pour s'assurer que le même individu n'est pas déjà enregistré et que l'individu est unique dans le système. Des justificatifs sont alors émis

pour permettre aux individus d'authentifier leur identité auprès des parties prenantes. De nombreux systèmes nationaux d'identification numérique utilisent un modèle centralisé, dans lequel le gouvernement ou une entité désignée par lui est le seul fournisseur du système. D'autres ont adopté des modèles fédérés, et un nouveau mouvement préconise des identités auto-souveraines décentralisées qui permettent un contrôle individuel encore plus important.

Les transactions électroniques

Les transactions électroniques sont à la base de l'économie numérique

L'économie numérique englobe et dépend d'activités économiques mises en œuvre au moyen de technologies et de services numériques.[1] Nombre de ces activités reposent sur **les transactions électroniques:** l'utilisation de documents, de messages et d'enregistrements électroniques pour conclure des transactions qui étaient traditionnellement basées sur l'encre et le papier. Les cadres juridiques qui soutiennent les transactions électroniques traduisent les concepts juridiques conventionnels essentiels à la conduite du commerce, comme ce qui constitue un document papier « original » ou le moment de la réception d'une offre de contrat sur papier, en équivalents électroniques.[2] Cela fournit des normes, une certitude et des recours aux parties qui font des affaires par le biais de transactions électroniques.

Signatures électroniques

De nombreuses actions commerciales et autres actions légales nécessitent la **signature** d'une ou plusieurs parties pour être considérées comme juridiquement valables. Au sens le plus large, une signature est le nom ou la marque d'un individu qui établit un lien entre l'individu et un élément signé. Elle permet à d'autres d'identifier la personne, de vérifier l'authenticité de l'objet signé et de confirmer le lien entre les deux.[3] Une **signature manuscrite** fait référence au moyen traditionnel d'appliquer de l'encre sur un document papier pour générer une signature.

Dans le contexte des transactions électroniques, les signatures manuscrites sont souvent peu pratiques, car elles augmentent les coûts de transaction et entravent la rapidité qui inspire souvent leur attrait. **Une signature électronique** - qui fait largement référence à l'utilisation de données sous forme électronique pouvant être associées à un document ou à un enregistrement et servir de preuve de l'intention de l'individu de signer - offre une alternative au site signature manuscrite. Il existe un large éventail de signatures électroniques, dont les plus simples consistent à apposer son nom au bas d'un courriel ou à prendre un scan numérique d'une signature manuscrite.[4] Les cadres juridiques soutiennent généralement l'utilisation des signatures électroniques en garantissant qu'une signature n'est pas privée d'effet juridique, de validité ou de force exécutoire uniquement en raison de sa forme électronique.[5] Cependant, ces cadres excluent souvent certaines transactions, notamment celles qui sont hautement personnelles ou soumises à des exigences légales existantes. Par exemple, la loi américaine ESIGN exclut spécifiquement les documents régis par la loi qui concernent les testaments, les codicilles, les fiducies testamentaires et les questions de droit de la famille, comme l'adoption ou le divorce.[6]

Signatures numériques

Toutes les signatures électroniques ne sont pas égales et le type de signature électronique peut avoir une incidence sur sa valeur probante pour établir le lien entre la personne et l'élément signé. Une **signature numérique** est un sous-ensemble de signatures électroniques doté de fonctions de sécurité supplémentaires. Les signatures numériques utilisent généralement **infrastructure à clé publique (ICP)** un type de cryptage impliquant une paire de « clés » de cryptage, l'une publique et l'autre privée. Lorsqu'une personne appose une signature numérique sur un document, elle utilise une clé privée unique, connue d'elle seule, pour le chiffrer.

Cette clé privée est associée à une clé publique unique, que la personne peut partager avec d'autres et qui est utilisée par le destinataire pour déchiffrer la signature numérique. Comme les deux clés sont associées l'une à l'autre et à aucune autre, lorsqu'on parvient à déchiffrer la signature numérique, on vérifie que la signature et le document auquel elle est attachée n'ont pas été modifiés depuis la création de la signature numérique.

De plus, lorsqu'une signature numérique est créée, un **certificat numérique** Les certificats numériques sont émis par des **autorités de certification**.[7] Les certificats numériques sont émis par des entités de confiance qui sont souvent expressément reconnues ou accréditées dans les cadres juridiques nationaux.[8] Le signataire doit s'enregistrer auprès de l'autorité de certification, en liant son identité à la clé publique. En réussissant à décrypter une signature numérique et en recevant un certificat numérique d'une autorité de certification de confiance, le destinataire a l'assurance que la signature et le document n'ont pas été altérés et que le signataire est bien la personne qu'il prétend être.

De nombreux cadres juridiques reconnaissent la différence entre la fiabilité des signatures électroniques de base et des signatures numériques, certains allant même jusqu'à stratifier davantage les sous-types de signatures numériques. Par exemple, le règlement eIDAS de l'UE reconnaît les signatures électroniques de base, les « signatures électroniques avancées » (qui sont similaires aux signatures numériques) et les « signatures électroniques qualifiées », qui offrent le plus haut niveau d'assurance et sont des signatures numériques accompagnées d'un certificat délivré par une entité spécifiquement certifiée à cette fin et créées à l'aide d'un type particulier de dispositif. Ce n'est qu'en ce qui concerne les signatures électroniques qualifiées que tous les États membres sont tenus d'assurer l'équivalence juridique entre les signatures manuscrites et les signatures électroniques.[9]

Systèmes nationaux d'identification numérique

Une identification sûre et fiable pour soutenir l'économie numérique

Permettre aux parties de vérifier l'identité des autres est essentiel pour garantir la sécurité et la fiabilité des transactions électroniques qui sont le moteur de l'économie numérique. Par exemple, les prêteurs doivent être sûrs que leurs prêts sont versés à la personne associée au dossier de crédit qu'ils ont examiné. De même, les consommateurs doivent être certains que le vendeur en ligne avec lequel ils effectuent une transaction est bien la personne qu'il prétend être. Même les certificats numériques qui prennent en charge les signatures numériques

exigent en fin de compte que le signataire s'enregistre et s'identifie auprès de l'autorité de certification.

En 2018, on estimait à 1 milliard le nombre d'individus dépourvus de documents d'identité de base, principalement en Afrique subsaharienne et en Asie du Sud.[10] En raison de normes sociales sexuées et d'exigences de demande disparates (telles que des exigences supplémentaires en matière de documents ou de signatures pour les femmes mariées), les femmes rencontrent davantage d'obstacles pour obtenir des documents d'identité officiels.[11] En conséquence, 45 % des femmes de plus de 15 ans dans les pays à faible revenu n'ont pas de pièce d'identité, contre 30 % des hommes.[12] Sur les quelque 1,7 milliard de personnes qui n'avaient pas de compte bancaire en 2017, près de 20 % l'attribuaient à l'absence de documents d'identité.[13] Une femme sur deux dans les économies à faible revenu ne dispose pas d'une carte d'identité nationale ou d'une pièce d'identité similaire, selon l'enquête ID4D-Findex.[14] En outre, les réfugiés, les apatrides, les personnes handicapées et les personnes vivant dans des zones rurales et reculées sont souvent confrontés aux plus grands obstacles pour obtenir des pièces d'identité officielles.[15] En réponse, la cible 16.9 de l'Objectif de développement durable 16 des Nations Unies vise à "fournir une identité légale à tous, y compris l'enregistrement des naissances" d'ici 2030.[16]

Qu'est-ce qu'un système d'identification ?

L'identité d'un individu **identité** est un ensemble d'attributs qui décrivent de manière unique cet individu dans un contexte donné.[17] Dans ce contexte, **unicité** signifie qu'un seul individu peut revendiquer une identité et que chaque individu ne peut revendiquer qu'une seule identité.[18] Par exemple, le nom et la date de naissance d'un individu sont probablement suffisants pour établir l'identité unique de cet individu au sein d'une petite communauté. Toutefois, dans un pays très peuplé où certains noms sont courants, ces seuls attributs peuvent être insuffisants pour établir l'unicité. Lorsque les attributs d'identité sont stockés et capturés électroniquement ou lorsqu'ils sont utilisés dans le cadre de services numériques ou de transactions électroniques, ils peuvent être considérés comme une **identité numérique**.[19] Un **système d'identification numérique** utilise la technologie numérique pour toutes les fonctions du système, de la capture et du stockage des données aux utilisations d'une identité numérique par les individus.[20]

Les systèmes d'identification administrés ou soutenus par les gouvernements se divisent souvent en deux catégories, **les systèmes d'identification fondamentaux** qui établissent une identité numérique de base et fournissent une identification à la population générale pour une grande variété de transactions et de services (par exemple, les systèmes nationaux d'identification et d'enregistrement civil), et **les systèmes d'identification fonctionnels**, qui répondent aux besoins spécifiques d'un secteur ou d'un cas d'utilisation particulier (par exemple, les systèmes de permis de conduire et d'inscription des électeurs).[21] La distinction n'est pas toujours nette. En l'absence d'un système d'identification fondamental approprié, un système d'identification fonctionnel peut évoluer et jouer un rôle plus fondamental. Par exemple, les numéros de sécurité sociale des États-Unis étaient à l'origine utilisés exclusivement pour suivre les revenus en vue de l'éligibilité à la sécurité

sociale, mais ils sont aujourd'hui utilisés à de nombreuses fins, telles que le recouvrement des impôts, l'évaluation des crédits et les transactions financières.[22] Les obstacles contextuels à l'accès aux pièces d'identité de base posant des exigences restrictives pour l'enregistrement, telles que la nécessité de présenter un témoin, une preuve d'adresse permanente et des exigences strictes pour la mise à jour des données (par exemple, les changements de nom de famille après un mariage)[23] peuvent exclure les populations vulnérables.

En permettant la preuve de l'identité, les systèmes d'identification numérique peuvent donner des moyens d'action et faciliter l'accès aux services financiers, sanitaires et sociaux de base.[24] Du côté de l'offre, les entreprises, les gouvernements et d'autres institutions peuvent bénéficier d'une baisse des coûts d'embarquement des utilisateurs ou des clients, d'une réduction des pertes dues à la fraude à l'identité et d'un accès à un bassin de main-d'œuvre plus large.[25] Les gouvernements peuvent aussi potentiellement bénéficier d'une augmentation des revenus grâce à une collecte des impôts plus efficace, précise et inclusive[26] et à une distribution plus transparente, précise et efficace des subventions. Par exemple, le gouvernement du Nigéria a intégré l'identification numérique dans son système de paie pour les officiers de police et a éliminé plus de 80 000 « officiers fantômes », comptes fictifs qui percevaient indûment des salaires.[27]

Systèmes nationaux d'identification numérique

Les systèmes nationaux d'identification numérique sont fondateurs par nature et mis en œuvre par, ou sous les auspices, du gouvernement.[28] Ils sont généralement disponibles pour la population générale locale, y compris les citoyens et les résidents à long terme, ainsi que les citoyens vivant à l'étranger. Cependant, certains systèmes limitent l'éligibilité aux seuls citoyens, comme la carte Omang du Botswana.[29]

Le grand nombre de personnes dépourvues de pièces d'identité dans les pays à faible revenu est souvent attribué au mauvais fonctionnement des systèmes d'enregistrement des faits d'état civil ou des systèmes nationaux d'identification sur papier.[30] Aujourd'hui, la technologie nécessaire pour soutenir et mettre en œuvre un système national d'identification numérique est devenue de plus en plus abordable, permettant à de nombreux pays à faible revenu de sauter les systèmes sur papier.[31] Il n'est pas surprenant que la mise en œuvre de systèmes nationaux d'identification numérique dans les pays à faible revenu et les pays développés se soit généralisée.[32]

Toutefois, comme toutes les nouvelles technologies, les systèmes nationaux d'identification numérique présentent des inconvénients potentiels. La vaste collecte de données personnelles sensibles ouvre la voie à des abus, tels que la surveillance par les gouvernements ou les entreprises et la discrimination à l'encontre des minorités vulnérables[33] Leur nature numérique les rend également vulnérables aux cyberattaques et autres risques liés à la sécurité des données. Comme les systèmes d'identification traditionnels, ils peuvent exclure volontairement ou par inadvertance les groupes marginalisés.

Pour minimiser ces risques, les organisations internationales ont développé de bonnes pratiques et des garanties pour la conception

et la mise en œuvre des systèmes nationaux d'identification numérique. Il s'agit notamment de s'assurer qu'un système est inclusif, c'est-à-dire qu'il est universellement accessible à une population et exempt de discrimination ou d'autres obstacles indus à l'enregistrement et à l'utilisation.[34] En outre, comme ces systèmes impliquent la collecte et la génération de grandes quantités de données personnelles, il est essentiel de disposer de cadres appropriés en matière de protection des données, de cybersécurité et de sécurité des données (voir les documents d'information sur la Protection des données et Cybersécurité et sécurité des données).[35]

Comment fonctionnent les systèmes nationaux d'identification numérique ?

Inscription

L'enregistrement dans un système national d'identification numérique peut être explicitement obligatoire, ce qui signifie qu'il existe une obligation légale de s'enregistrer. Par exemple, la loi sur le système d'identification des Philippines exige que chaque citoyen et résident s'enregistre auprès de PhilSys, le système national d'identification numérique du pays.[36] D'autres systèmes sont ostensiblement volontaires mais deviennent implicitement obligatoires parce que l'enregistrement est nécessaire pour accéder aux services publics de base. Par exemple, l'enregistrement pour la carte d'identité nationale du Pakistan est volontaire, mais une carte est nécessaire pour ouvrir un compte bancaire, obtenir un passeport ou un raccordement au gaz ou à l'électricité, payer une facture de services publics ou effectuer une transaction avec l'État.[37] Le fait de lier directement un système d'identification numérique à l'accès aux services publics et privés peut inciter à l'adoption de l'identification numérique, mais en l'absence de garanties appropriées, une telle exigence pourrait priver les populations mal desservies de services importants, en particulier dans les pays où l'écosystème de l'identification numérique est en phase d'émergence. [38]

Le processus commence généralement par la collecte des attributs des individus qui seront utilisés pour établir une identité numérique. Ces attributs peuvent comprendre **données biographiques**, comme le nom, la date de naissance, le sexe, l'adresse et **données biométriques**, comme les empreintes digitales, les scans de l'iris, les images faciales et les signatures. En 2018, quelque 83 pays collectaient des données biométriques (empreintes digitales ou iris) dans le cadre d'un système d'identification fondamental.[39] Des critiques se sont opposés à la collecte obligatoire de données biométriques, arguant que les individus ne devraient pas être tenus de placer leurs données biométriques sensibles et immuables à risque de divulgation ou d'utilisation abusive lorsque des approches alternatives existent.[40]

Une fois collectées, les données biographiques sont généralement **validé** pour s'assurer que l'individu est bien la personne qu'il prétend être. Les techniques de validation consistent souvent à fournir des documents d'identification existants, tels qu'un acte de naissance ou un passeport. Dans les populations où l'absence de tels documents est courante, des attestations de membres de la communauté peuvent être exigées. Par exemple, en Tanzanie, une liste de personnes avec photos peut être affichée dans une communauté pour permettre aux membres du public d'aider à corriger des informations inexactes.

Les demandes peuvent également être examinées par des « comités de sécurité de village et de district », qui comprennent des représentants de diverses agences, y compris le département de l'immigration, la police et le gouvernement local.[41] Une fois l'identité d'un individu validée, un système utilise généralement des techniques de **déduplication** pour s'assurer que le même individu n'est pas déjà enregistré. Les technologies de reconnaissance des données biométriques sont considérées comme les techniques de déduplication les plus précises.[42]

Les conditions d'enregistrement peuvent être particulièrement difficiles à remplir pour les femmes. La présentation d'un témoin pour obtenir une carte d'identité nationale peut être un défi pour les femmes dans certains contextes socioculturels, en particulier lorsque les points d'enregistrement sont limités et que les femmes doivent également couvrir les frais de déplacement d'un témoin. De même, les cartes d'identité fonctionnelles peuvent être plus accessibles aux hommes, tandis que les cartes d'identité temporaires de base peuvent être plus accessibles aux femmes si elles se trouvent à proximité du domicile de la femme (par exemple, une déclaration sous serment d'un ancien du village). Au Nigeria, 12 % des hommes (âgés de plus de 15 ans) possèdent un permis de conduire, contre 1 % des femmes. L'intégration limitée des bases de données d'identité fondamentales et fonctionnelles peut exacerber les difficultés d'enregistrement. Par exemple, une femme peut avoir besoin de la permission de son mari ou de son père pour se déplacer chaque fois qu'elle doit demander une carte d'identité, recevoir des justificatifs, mettre à jour ou renouveler des justificatifs, ou demander un service spécifique. En outre, les femmes peuvent être moins alphabétisées que les hommes et donc moins susceptibles d'avoir les compétences nécessaires pour s'orienter dans le processus de demande ou pour comprendre l'intérêt d'une carte d'identité numérique pour elles-mêmes et leurs enfants. Enfin, les femmes peuvent également rencontrer des obstacles juridiques à l'enregistrement lorsque les politiques relatives à l'identification manquent de spécificité ou contiennent des dispositions sexistes. Par exemple, en Papouasie-Nouvelle-Guinée, la loi établit que le père est la « personne responsable » de la modification des pièces d'identité d'un enfant (sauf s'il est décédé ou s'il n'en a pas la garde), ce qui peut limiter la capacité d'une mère à effectuer les mises à jour ou les modifications nécessaires au nom de l'enfant.[43]

Délivrance des lettres de créance

Une fois qu'une personne est enregistrée dans un système national d'identification numérique, elle se voit généralement livrer un **justificatif** : un document, un objet ou une structure de données qui atteste de son identité.[44] Les numéros d'identification uniques et les cartes d'identité physiques (souvent enrichies de puces électroniques, de codes-barres ou de codes QR lisibles par machine) sont des formes traditionnelles de justificatifs, mais les justificatifs numériques basés sur des applications ou des cartes SIM mobiles sont de plus en plus courants. Par exemple, le système national d'identification de la Moldavie attribue à chaque citoyen un numéro d'identification personnel à 13 chiffres à la naissance, livre une carte physique et propose un justificatif basé sur la carte SIM.[45]

Dans certaines circonstances, les femmes peuvent ne pas avoir le plein contrôle de

leurs titres d'identité. Par exemple, des recherches ont montré que parfois, la belle-famille des femmes ou les agences pour l'emploi prennent leurs pièces d'identité, limitant ainsi leur liberté de mouvement.[46]

Cas d'utilisation

L'un des principaux cas d'utilisation d'un système d'identification est **l'authentification**: le processus consistant à prouver qu'un individu enregistré est bien la personne qu'il prétend être. Dans un système numérique, l'authentification est réalisée en présentant un ou plusieurs facteurs d'authentification pour affirmer l'identité de l'individu, qui sont vérifiés électroniquement. Généralement, ces facteurs comprennent quelque chose d'inhérent à la personne (par exemple, une biométrie comme une empreinte digitale ou un scan de l'iris), quelque chose qu'une personne connaît (par exemple, un mot de passe ou un code PIN), ou quelque chose qu'une personne possède (par exemple, un justificatif physique ou électronique).[47] Pour renforcer l'authentification, de nombreux systèmes exigent l'utilisation de plusieurs facteurs. Une fois authentifié, un **partie fiable** - fournisseur de services du secteur public ou privé qui utilise le système pour authentifier les personnes - a un degré élevé d'assurance qu'il communique ou effectue une transaction avec la bonne personne. L'authentification peut donc être utilisée pour soutenir les transactions électroniques.

Certains systèmes d'identification numérique comprennent autorisation une fonctionnalité qui permet au système d'identification de communiquer aux parties concernées si un individu possède un attribut particulier. Par exemple, un système peut confirmer qu'un individu est suffisamment âgé pour bénéficier d'un avantage gouvernemental particulier. D'autres systèmes comprennent **attribution** une fonctionnalité qui permet aux individus d'utiliser le système pour générer des signatures contraignantes, souvent à l'aide de signatures numériques.[48]

Modèles et institutions

De nombreux pays qui ont mis en œuvre des systèmes nationaux d'identification numérique utilisent un **modèle centralisé**, dans lequel le gouvernement ou une entité désignée par lui agit en tant que fournisseur unique d'un système national d'identification.[49] Il s'agit du modèle utilisé par le système Aadhaar de l'Inde (exploité par la Unique Identification Authority of India)[50] et le système d'identification national du Nigeria (exploité par la National Identity Management Commission).[51] Ces entités peuvent faire partie d'un ministère/département existant ou d'autorités autonomes et indépendantes. Elles peuvent assumer la responsabilité de la mise en œuvre du système, notamment en procédant à l'enregistrement, en livrant des justificatifs d'identité, en certifiant les parties fiables et en recevant et en traitant les plaintes des utilisateurs.

Certains détracteurs des systèmes nationaux centralisés d'identification numérique affirment qu'ils empêchent la concurrence entre plusieurs systèmes, qui pourrait conduire à une plus grande efficacité et à de meilleurs résultats pour les utilisateurs.[52] D'autres pays s'appuient sur un **modèle fédéré**, dans lequel plusieurs entités accréditées par le gouvernement peuvent fournir une identité numérique reconnue par le gouvernement.[53] Par exemple, le système GOV.UK Verify du Royaume-Uni utilise des entreprises privées certifiées qui sont tenues de suivre des procédures et des

normes prescrites en tant que fournisseurs d'identité.[54]

Divers mécanismes sont utilisés pour financer les systèmes nationaux d'identification numérique. Certains sont financés directement par les gouvernements ou avec l'aide d'organisations donatrices. D'autres font appel à des partenariats avec des fournisseurs du secteur privé. Les frais d'utilisation peuvent également soutenir ces systèmes. Bien que les frais d'enregistrement soient généralement déconseillés, car ils peuvent constituer un obstacle à l'inclusion, ils peuvent être imposés aux personnes qui souhaitent obtenir des services accélérés ou le remplacement d'informations d'identification perdues, ou aux parties utilisatrices pour l'utilisation de la fonctionnalité d'authentification.

Questions émergentes

Identité auto-souveraine

Certains critiques ont fait valoir que les systèmes nationaux d'identification numérique mis en œuvre par les gouvernements se sont révélés dépourvus de contrôles de la vie privée, vulnérables aux cyberattaques et largement incompatibles les uns avec les autres.[55] En particulier, certains ont cité une violation des données du système Aadhaar de l'Inde en 2018, qui a entraîné le vol des données personnelles de plus d'un milliard de personnes, comme preuve de l'insécurité inhérente à tout système centralisé.[56]

En réponse à cette situation, un mouvement s'est formé, prônant l'utilisation d'une **identité auto-souveraine** (SSI), un cadre qui envisage un système de gestion d'identité décentralisé fonctionnant indépendamment d'acteurs publics tiers et donnant la priorité à la sécurité, à la vie privée, à l'autonomie individuelle et à l'auto-responsabilisation.[57] La SSI repose sur la conviction qu'un individu doit posséder et contrôler son identité numérique sans l'intervention d'autorités administratives.[58]

Tel qu'il est envisagé, le SSI est rendu possible par **portefeuilles numériques** disponibles sur les appareils mobiles, qui peuvent être utilisés pour stocker et gérer des justificatifs numériques tels que des passeports numériques, des diplômes numériques et des titres de propriété numériques. Ces justificatifs sont accessibles à l'utilisateur individuel, qui est le seul à pouvoir déterminer avec qui ils doivent être partagés et l'étendue de ce partage. Par exemple, une personne peut prouver qu'elle a plus de 21 ans sans avoir à révéler son âge réel, contrairement à la présentation d'une pièce d'identité classique. Comme les justificatifs numériques sont disponibles dans un portefeuille numérique, ils sont entièrement portables et facilement disponibles.[59]

Le SSI repose sur l'utilisation de la **technologie du registre distribué (TRD)** la technologie qui sous-tend la blockchain. Lorsque des certificats numériques sont émis, une preuve chiffrée de l'émission (et non le certificat lui-même) est enregistrée dans un registre virtuel décentralisé, avec un horodatage et la signature numérique de l'émetteur. Les registres eux-mêmes sont immuables et toute mise à jour du statut de l'entrée - par exemple, si le titre est révoqué - est également enregistrée dans le registre. Lorsqu'un justificatif numérique est présenté à un tiers, celui-ci peut facilement consulter les entrées du registre pour en vérifier l'authenticité.[60]

En raison de la nature décentralisée de la SSI, les identités numériques restent portables et interopérables sur de multiples plates-formes.[61] De plus, comme aucune autorité centralisée ne gère le processus d'authentification, il n'est pas possible de suivre et d'enregistrer l'utilisation des identifiants numériques par l'individu, ce qui élimine les préoccupations concernant la surveillance indésirable des gouvernements ou des entreprises.

Ressources supplémentaires

Autres lectures

- Mason, Stephen, Electronic Signatures in Law: Fourth Edition (anglais)
- CNUDCI, Loi type de la CNUDCI sur le commerce électronique (1996)
- CNUDCI, Loi type de la CNUDCI sur les signatures électroniques (2001)
- World Bank Group, ID4D, Practitioner's Guide (anglais)
- World Bank Group, ID4D, ID Enabling Environment Assessment (IDEEA) Guidance Note (anglais)
- ITU, Digital identity in the ICT ecosystem: An overview (anglais)

Organisations

- Banque mondiale, ID4D, Identification pour le développement
- Access Now
- Autorité indienne d'identification unique
- Commission nationale de gestion de l'identité (Nigeria)

Références

[1] Voir OCDE, A Roadmap toward a Common Framework for Measuring the Digital Economy, Rapport pour le groupe de travail du G20 sur l'économie numérique (2020), p. 34, reconnaissant l'absence de définition commune et proposant la suivante : "L'économie numérique englobe toute activité économique qui dépend de l'utilisation d'intrants numériques, y compris les technologies numériques, l'infrastructure numérique, les services et les données numériques, ou qui est considérablement améliorée par cette utilisation. Elle fait référence à tous les producteurs et consommateurs, y compris les pouvoirs publics, qui utilisent ces intrants numériques dans leurs activités économiques." Disponible à l'adresse https://www.oecd.org/going-digital/topics/measurement/.

[2] Voir la Loi type de la CNUDCI sur le commerce électronique avec le Guide pour son incorporation 1996. Disponible à l'adresse https://uncitral.un.org/en/texts/ecommerce.

[3] Determann, Loretta, "Electronic Form Over Substance : eSignature Laws Need Upgrades", Hastings Law Journal Vol 72:1385 (mai 2021). Disponible à l'adresse https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3436327.

[4] Determann, Loretta, "Electronic Form Over Substance : eSignature Laws Need Upgrades", Hastings Law Journal Vol 72:1385 (mai 2021). Disponible à l'adresse https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3436327.

[5] Voir, par exemple, la loi américaine sur les signatures électroniques dans le commerce mondial et national, 2000, §106 ; la loi saoudienne sur les transactions électroniques, 2007, Art 5 ; le règlement UE n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques dans le marché intérieur et abrogeant la directive 1999/93/CE, Art 25.

[6] Au §103.

[7] Les certificats numériques ont d'autres utilisations que les signatures numériques, notamment la sécurisation des transactions par carte de crédit, des transferts de données et de la navigation sur Internet.

[8] Par exemple, la loi sur les transactions électroniques et la cybersécurité du Malawi, 2016, §51 accorde à l'Autorité de régulation des communications du Malawi le pouvoir d'accréditer des " autorités de certification. "

[9] Règlement UE n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques dans le marché intérieur et abrogeant la directive 1999/93/CE, articles 3, 25, 26 & 32.

[10] Groupe de la Banque mondiale, ID4D, Guide du praticien, version 1.0 (octobre 2019), à l'adresse 1. Disponible sur https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[11] Dahan & Hanmer, Le programme d'identification pour le développement (ID4D) : son potentiel pour l'autonomisation des femmes et des filles p. 12-13.

[12] Institut mondial McKinsey, Identification numérique : A Key to Inclusive Growth, Summary of Findings (janvier 2019), p. 3. Disponible à l'adresse https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/The%20value%20of%20digital%20ID%20for%20the%20global%20economy%20and%20society/MGI-Digital-identification-A-key-to-inclusive-growth.pdf.

[13] Institut mondial McKinsey, Identification numérique : A Key to Inclusive Growth, Summary of Findings (janvier 2019), p. 3. Disponible à l'adresse https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/The%20value%20of%20digital%20ID%20for%20the%20global%20economy%20and%20society/MGI-Digital-identification-A-key-to-inclusive-growth.pdf.

[14] Voir Groupe de la Banque mondiale, Inclusive and trusted digital ID can unlock opportunities for the World's most vulnerable, (août 2019). Disponible à l'adresse https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable.

[15] Voir Groupe de la Banque mondiale, Inclusive and trusted digital ID can unlock opportunities for the World's most vulnerable, (août 2019). Disponible à l'adresse https://www.worldbank.org/en/news/immersive-story/2019/08/14/inclusive-and-trusted-digital-id-can-unlock-opportunities-for-the-worlds-most-vulnerable.

[16] Voir le site Web des Nations unies, Département des affaires économiques et sociales, Développement durable, les 17 objectifs. Disponible sur https://sdgs.un.org/goals.

[17] Basé sur la définition du Groupe de la Banque mondiale, ID4D, Guide du praticien, version 1.0 (octobre 2019), à Glossaire. Disponible à l'adresse https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[18] Voir Groupe de la Banque mondiale, ID4D, Practitioner's Guide, Version 1.0 (octobre 2019), à l'adresse 4. Disponible à l'adresse https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[19] Voir, Groupe de la Banque mondiale, ID4D, Guide du praticien, version 1.0 (octobre 2019), à l'adresse Glossaire. Disponible à l'adresse https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide. Voir également, UIT, L'identité numérique dans l'écosystème des TIC : Une vue d'ensemble (2018), à l'adresse 5. Disponible à l'adresse https://www.itu.int/pub/D-PREF-BB.ID01-2018.

[20] Adapté du Groupe de la Banque mondiale, ID4D, Guide du praticien, version 1.0 (octobre 2019), à Glossaire. Disponible à l'adresse https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[21] Voir, UIT, L'identité numérique dans l'écosystème des TIC : Une vue d'ensemble (2018), à l'adresse vi. Disponible à l'adresse https://www.itu.int/pub/D-PREF-BB.ID01-2018. Voir également, Groupe de la Banque mondiale, ID4D, Guide du praticien, version 1.0 (octobre 2019), à l'adresse 12. Disponible à l'adresse https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[22] Groupe de la Banque mondiale, ID4D, Note d'orientation sur l'évaluation de l'environnement favorable à l'ID (IDEEA) (2018), p. 10-11. Disponible à l'adresse https://id4d.worldbank.org/legal-assessment.

[23] GSMA.com, disponible à l'adresse https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/04/Exploring-the-Gender-Gap-in-Identification-Policy-Insights-from-10-Countries-Web.pdf.

[24] Groupe de la Banque mondiale, ID4D, Guide du praticien, version 1.0 (octobre 2019), à l'adresse 3. Disponible sur https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[25] Institut mondial McKinsey, Identification numérique : Une clé pour une croissance inclusive, résumé des conclusions (janvier 2019), à la page 12. Disponible sur https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/The%20value%20of%20digital%20ID%20for%20the%20global%20economy%20and%20society/MGI-Digital-identification-A-key-to-inclusive-growth.pdf.

[26] Institut mondial McKinsey, Identification numérique : Une clé pour une croissance inclusive, résumé des conclusions (janvier 2019), à la page 13. Disponible sur https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/The%20value%20of%20digital%20ID%20for%20the%20global%20economy%20and%20society/MGI-Digital-identification-A-key-to-inclusive-growth.pdf.

[27] Udo, Bassey, " Over 80,000 'ghost officers' uncovered in Nigerian Police ", Premium Times (26 mars 2018). Disponible à l'adresse https://www.premiumtimesng.com/news/headlines/263052-over-80000-ghost-officers-uncovered-in-nigerian-police.html.

[28] Voir, Groupe de la Banque mondiale, ID4D, Note d'orientation sur l'évaluation de l'environnement favorable à l'ID (IDEEA) (2018), à la page 9. Disponible sur https://id4d.worldbank.org/legal-assessment.

[29] Voir le site Web de la République du Botswana, National ID Card Application. Disponible à l'adresse https://www.gov.bw/civil-registration/national-identity-card-application.

[30] Groupe de la Banque mondiale, ID4D, Guide du praticien, version 1.0 (octobre 2019), à l'adresse 1. Disponible sur https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[31] Institut mondial McKinsey, Identification numérique : A Key to Inclusive Growth, Summary of Findings (janvier 2019), p. 5. Disponible à l'adresse https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/The%20value%20of%20digital%20ID%20for%20the%20global%20economy%20and%20society/MGI-Digital-identification-A-key-to-inclusive-growth.pdf.

[32] Voir le site du World Privacy Forum, National IDs Around the World - Interactive map. Disponible à l'adresse https://www.worldprivacyforum.org/2017/07/national-ids-around-the-world/.

[33] Voir, par exemple, Guo & Noori, This is the real story of the Afghan biometric databases abandoned to the Taliban (août 2021).

[34] Outre la réduction des obstacles traditionnels à l'accès, tels que la distance et le coût, les gouvernements devront peut-être s'engager activement auprès des groupes historiquement marginalisés pour garantir une adoption équitable des services d'identité numérique. Voir Banque mondiale, Inclusive and trusted digital ID can unlock opportunities for the World's most vulnerable (août 2019).

[35] Voir, par exemple, Groupe de la Banque mondiale, Principes d'identification pour le développement durable : Vers l'ère numérique - Deuxième édition (mars 2021). Disponible à l'adresse https://documents.worldbank.org/en/publication/documents-reports/documentdetail/213581486378184357/principles-on-identification-for-sustainable-development-toward-the-digital-age.

[36] Loi sur le système d'identification philippin, loi de la République n° 11055, 24 juillet 2017, au §9. Disponible sur https://neda.gov.ph/philsys/.At §9

[37] Groupe de la Banque mondiale, ID4D, Note d'orientation sur l'évaluation de l'environnement favorable à l'ID (IDEEA) (2018), à 51. Disponible à l'adresse https://id4d.worldbank.org/legal-assessment.

[38] Par exemple, une étude menée à Jharkhand, en Inde, a révélé que le fait d'exiger des bénéficiaires de subventions alimentaires qu'ils relient leur numéro Aadhaar à leur compte a entraîné une réduction des prestations pour 23 % des bénéficiaires. Muralidharan et al., Balancing corruption and exclusion : Incorporating Aadhaar into PDS (2020).

[39] UIT, L'identité numérique dans l'écosystème des TIC : An overview (2018), à la page 3, disponible à l'adresse https://www.itu.int/pub/D-PREF-BB.ID01-2018.

[40] Voir, par exemple, Access Now, National Digital Identity Programmes : What's Next ? (mai 2018), p. 6, disponible à l'adresse https://www.accessnow.org/accessnow-digital-id-paper.

[41] Groupe de la Banque mondiale, L'état des systèmes d'identification en Afrique : Une synthèse des évaluations par pays, 2017 à la page 41. Disponible à l'adresse http://documents.worldbank.org/curated/en/156111493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDDAssessments-PUBLIC.pdf. Voir également, Groupe de la Banque mondiale, ID4D, Note d'orientation sur l'évaluation de l'environnement favorable à l'identification (IDEEA) (2018), à 58-59. Disponible à l'adresse https://id4d.worldbank.org/legal-assessment.

[42] Groupe de la Banque mondiale, ID4D, Guide du praticien, version 1.0 (octobre 2019), p. 154-155. Disponible à l'adresse https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[43] GSMA, Explorer l'écart entre les sexes dans l'identification : Aperçu des politiques de 10 pays (2019). Disponible à l'adresse suivante : Source : https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/04/Exploring-the-Gender-Gap-in-Identification-Policy-Insights-from-10-Countries-Web.pdf

[44] Groupe de la Banque mondiale, ID4D, Guide du praticien, version 1.0 (octobre 2019), p. 157. Disponible à l'adresse https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[45] Groupe de la Banque mondiale, ID4D, Guide du praticien, version 1.0 (octobre 2019), p. 166. Disponible à l'adresse https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide.

[46] Bailur & Smertnik, When ID works for women : Quel est le rôle de l'identification pour aider les femmes à accéder au travail ? (mars 2019).

[47] Voir, Groupe de la Banque mondiale, ID4D, Guide du praticien, version 1.0 (octobre 2019), p. 170. Disponible à l'adresse https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide. Voir également, Groupe de la Banque mondiale, ID4D, Note d'orientation sur l'évaluation de l'environnement favorable à l'ID (IDEEA) (2018), à 37. Disponible à l'adresse https://id4d.worldbank.org/legal-assessment.

[48] Groupe de la Banque mondiale, ID4D, Note d'orientation sur l'évaluation de l'environnement favorable à l'ID (IDEEA) (2018), p. 38-39. Disponible à l'adresse https://id4d.worldbank.org/legal-assessment.

[49] Voir, Groupe de la Banque mondiale, ID4D, Guide du praticien, version 1.0 (octobre 2019), p. 16-17. Disponible à l'adresse https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide. Voir également, UIT, L'identité numérique dans l'écosystème des TIC : An overview (2018), à l'adresse 5, disponible à l'adresse https://www.itu.int/pub/D-PREF-BB.ID01-2018.

[50] Voir le site web de l'Autorité indienne d'identification unique. Disponible à l'adresse https://uidai.gov.in/.

[51] Voir le site de la Commission nationale de gestion de l'identité. Disponible à l'adresse https://nimc.gov.ng/.

[52] Voir, par exemple, Access Now, National Digital Identity Programmes : What's Next ? (mai 2018), p. 6 et 34. Disponible à l'adresse https://www.accessnow.org/accessnow-digital-id-paper.

[53] Voir, Groupe de la Banque mondiale, ID4D, Guide du praticien, version 1.0 (octobre 2019), p. 16-17. Disponible à l'adresse https://documents.worldbank.org/en/publication/documents-reports/documentdetail/248371559325561562/id4d-practitioner-s-guide. Voir également, UIT, L'identité numérique dans l'écosystème des TIC : An overview (2018), à l'adresse 5, disponible à l'adresse https://www.itu.int/pub/D-PREF-BB.ID01-2018.

[54] Groupe de la Banque mondiale, ID4D, Note d'orientation sur l'évaluation de l'environnement favorable à l'ID (IDEEA) (2018), à 67. Disponible à l'adresse https://id4d.worldbank.org/legal-assessment. Voir, site web UK.GOV Verify, Introducing UK.GOV Verify. Disponible à l'adresse https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify.

[55] Lim, Jonathan, "Self-Sovereign Identity : The Harmonising of Digital Identity Solutions through Distributed Ledger Technology", Australian National University Journal of Law and Technology Vol 1(2) (septembre 2020). Disponible à l'adresse https://anujolt.org/article/17432-self-sovereign-identity-the-harmonising-of-digital-identity-solutions-through-distributed-ledger-technology.

[56] Lim, Jonathan, "Self-Sovereign Identity : The Harmonising of Digital Identity Solutions through Distributed Ledger Technology", Australian National University Journal of Law and Technology Vol 1(2) (septembre 2020). Disponible à l'adresse https://anujolt.org/article/17432-self-sovereign-identity-the-harmonising-of-digital-identity-solutions-through-distributed-ledger-technology.

[57] Giannopoulou A & Wang F, "Self-sovereign identity", Internet Policy Review, 10(2) (2021). Disponible à l'adresse https://policyreview.info/glossary/self-sovereign-identity.

[58] López, Marcos Allende, Banque interaméricaine de développement, Self-Sovereign Identity, The Future of Identity : Auto-souveraineté, portefeuilles numériques et blockchain (2020). Disponible à l'adresse https://publications.iadb.org/publications/english/document/Self-Sovereign-Identity-The-Future-of-Identity-Self-Sovereignity-Digital-Wallets-and-Blockchain.pdf.

[59] López, Marcos Allende, Banque interaméricaine de développement, Self-Sovereign Identity, The Future of Identity : Auto-souveraineté, portefeuilles numériques et blockchain (2020). Disponible à l'adresse https://publications.iadb.org/publications/english/document/Self-Sovereign-Identity-The-Future-of-Identity-Self-Sovereignity-Digital-Wallets-and-Blockchain.pdf.

[60] López, Marcos Allende, Banque interaméricaine de développement, Self-Sovereign Identity, The Future of Identity : Auto-souveraineté, portefeuilles numériques et blockchain (2020). Disponible à l'adresse https://publications.iadb.org/publications/english/document/Self-Sovereign-Identity-The-Future-of-Identity-Self-Sovereignity-Digital-Wallets-and-Blockchain.pdf.

[61] Lim, Jonathan, "Self-Sovereign Identity : The Harmonising of Digital Identity Solutions through Distributed Ledger Technology", Australian National University Journal of Law and Technology Vol 1(2) (septembre 2020). Disponible à l'adresse https://anujolt.org/article/17432-self-sovereign-identity-the-harmonising-of-digital-identity-solutions-through-distribute d-ledger-technology

À propos de l'UNCDF

L'UN Capital Development Fund (UNCDF) facilite l'accès aux capitaux publics et privés par les populations les plus démunies dans les 46 pays les moins avancés du monde (PMA).

Dans le cadre de son mandat de fourniture de capitaux et d'instruments d'investissement, l'UNCDF offre des modèles de financement du «last mile» permettant de débloquer les ressources publiques et privées, notamment au niveau national, afin de réduire la pauvreté et d'encourager le développement économique local.

Les modèles de financement de l'UNCDF ouvrent à travers trois axes, à savoir : 1) les économies numériques inclusives, qui connectent les personnes, les ménages et les petites entreprises aux écosystèmes financiers qui catalysent la participation à l'économie locale et fournissent des outils pour vaincre la pauvreté et gérer leur vie financière ; 2) le financement du développement local, qui permet aux municipalités de dynamiser l'expansion économique locale et le développement durable par le biais de la décentralisation fiscale, du financement municipal innovateur et du financement structuré de projets ; et 3) le financement d'investissements, qui fournit une structuration financière catalytique, une réduction des risques et le déploiement des investissements pour favoriser l'impact des ODD et la mobilisation des ressources au niveau national.

L'UNCDF Policy Accelerator travaille avec les gouvernements pour les aider à créer des politiques et des réglementations qui incluent tout le monde dans l'économie numérique, partage des outils et des guides pratiques basés sur notre modèle d'assistance technique et nos ressources de référence, et fourni des bourses aux décideurs politiques et aux régulateurs pour qu'ils puissent étudier avec nos organisations partenaires de classe mondiale.

À propos de Macmillan Keck

Macmillan Keck Attorneys & Solicitors conseille ses clients en matière de stratégie, de plaidoyer, d'affaires controverses et réformes dans l'économie numérique. Les clients du cabinet comprennent des opérateurs de télécom les fournisseurs de services financiers numériques, les fournisseurs de services de santé et d'éducation en ligne fournisseurs de contenu, d'applications et de services numériques, des gouvernements et des autorités de régulation de la concurrence et des organisations internationales. Le cabinet a mené à bien de nombreux projets complexes dans une majorité de pays sur tous les continents.

Clause de non-responsabilité

Les appellations utilisées sur cette carte et la présentation des données qui y figurent n'impliquent aucune prise de position de la part du Secrétariat de l'Organisation des Nations Unies ou de l'UNCDF quant au statut juridique des pays, territoires, villes ou zones.

Cette publication a été révisée pour la dernière fois en Mars 2022.

Unlocking Public and Private Finance for the Poor

policy.accelerator@uncdf.org

policyaccelerator.uncdf.org | uncdf.org

FIND US