CATALOGUE DE

Normes techniques pour les systèmes d'identification numérique

ID4D
IDENTIFICATION FOR DEVELOPMENT

GROUPE DE LA BANQUE MONDIALE

1818 H Street NW
Washington D.C., 20433
Téléphone : 202-473-1000
Site Internet : www.worldbank.org

Cet ouvrage, initialement publié en anglais sous le titre *Catalog of Technical Standards for Digital Identification Systems*, a été établi par les services de la Banque mondiale avec la contribution de collaborateurs extérieurs. Les observations, interprétations et opinions qui y sont exprimées ne reflètent pas nécessairement les vues de la Banque mondiale, de son Conseil des Administrateurs ou des pays que ceux-ci représentent.

La Banque mondiale ne garantit pas l'exactitude des données contenues dans cet ouvrage. Les frontières, les couleurs, les dénominations et toute autre information figurant sur les cartes du présent ouvrage n'impliquent de la part de la Banque mondiale aucun jugement quant au statut juridique d'un territoire quelconque et ne signifient nullement que l'institution reconnaît ou accepte ces frontières.

TABLE DES MATIÈRES

LISTE DES FIGURES

ABRÉVIATIONS

AFNOR	Association française de normalisation
ANSI	American National Standard Institute (Institut américain de normalisation)
ASN.1	Abstract Syntax Notation One
BAPI	Biometric Application Programming Interface (Interface de programme d'application biométrique)
BM	Banque mondiale
CAP	Programme d'authentification CAP
CBEFF	Common Biometric Exchange Formats Framework (Cadre de formats d'échange biométriques communs)
CEI	Commission électrotechnique internationale
CEN	Comité européen de normalisation
CITeR	Center for Identification Technology Research
DHS	Department of Homeland Security (ministère de la Sécurité intérieure)
DIN	Institut de normalisation allemand
eID	Carte d'identité électronique
EMV	Europay, MasterCard et Visa— Norme de paiement par carte intelligente
EMVCo	EMV Company
FIDO	Fast IDentity Online (protocole d'authentification forte pour les paiements en ligne)
GSM	Global System for Mobile Communication (précédemment Groupe Spécial Mobile)
GSMA	GSM Association
IBIA	International Biometrics and Identification Association (Association internationale de l'identité biométrique)
ID	Identification
ID4D	Initiative Identification pour le développement (ID4D) du Groupe de la Banque mondiale
INCITS	Comité international pour les normes relatives aux technologies de l'information
ISO	Organisation internationale de normalisation
JTC	Comité technique mixte
NADRA	Service en charge de la base de données nationale et de l'enregistrement (Pakistan)
NICOP	Carte d'identité nationale pour les Pakistanais de l'étranger
NIST	Institut national des normes et de la technologie (États-Unis)
OACI	Organisation de l'aviation civile internationale
OASIS	Organization for the Advancement of Structural Information Standards (consortium mondial pour la normalisation et la standardisation de formats de fichiers ouverts)vi
ODD	Objectif de développement durable
OIT	Organisation internationale du travail
OpenID	Open ID Foundation
PIN	Numéro d'identification personnel

PKI	Infrastructure à clés publiques
PSA	Organisme pakistanais de normalisation
RFID	Radio-Frequency Identification (identification par radiofréquences)
RMG	Groupe de gestion des enregistrements
SA	Standards Australia (autorité australienne de normalisation)
SIA	Secure Identity Alliance
SIS	Institut suédois de normalisation
SNBA	Association nationale suédoise de biométrie
TI	Technologies de l'information
TIC	Technologies de l'information et des communications
UIDAI	Autorité indienne de l'identification unique
UIN	Numéro unique d'identification des personnes physiques
UIT-T	Secteur de la normalisation des télécommunications de l'Union internationale des télécommunications
WG	Groupe de travail
ZLA	Zone de lecture automatique

À PROPOS DE L'INITIATIVE ID4D

L'initiative Identification pour le développement (ID4D) du Groupe de la Banque mondiale mobilise les connaissances et savoir-faire de différents secteurs partout dans le monde, dans le but d'aider les pays à réaliser le potentiel transformationnel qu'offrent les systèmes d'identification numérique, et ainsi atteindre les Objectifs de développement durable. Mise en œuvre dans tout le Groupe de la Banque mondiale, l'initiative concerne les pratiques et unités mondiales, qui travaillent sur le développement numérique, la protection sociale, la santé, l'inclusion financière, la gouvernance, la parité hommes-femmes et les questions juridiques, entres autres.

L'initiative ID4D se fixe pour mission de donner à tous les individus les moyens d'accéder aux services et d'exercer leurs droits. Elle vise à cet effet à donner une forme officielle d'identification au plus grand nombre, en s'appuyant sur ses trois piliers : i) leadership avisé et analyses pour créer des données probantes et combler les lacunes de connaissances ; ii) plateformes et réunions de niveau international pour donner de l'ampleur aux bonnes pratiques, collaborer et renforcer la sensibilisation ; et iii) engagement national et régional pour apporter l'aide technique et financière nécessaire à la mise en œuvre de systèmes d'identification numérique fiables, inclusifs et responsables, intégrés aux données d'état-civil.

Les travaux de l'initiative ID4D sont rendus possibles avec le soutien du Groupe de la Banque mondiale, de la Fondation Bill & Melinda Gates, d'Omidyar Network et de l'État australien.

Pour en savoir plus sur l'initiative ID4D, visiter id4d.worldbank.org.

REMERCIEMENTS

Le catalogue a été préparé par Anita Mittal, avec des contributions de Tariq Malik, Ott Köstner, Flex Ortega De La Tora, Adam Cooper, Seth Ayers, Daniel Bachenheimer, Alastair Treharne, Dr Narjees Adennebi, Sanjay Dharwadker, Marta Ienco, Stéphanie de Labriolle et Dr Adeel Malik.

Le catalogue a été présenté lors de deux ateliers, organisés en septembre 2017 et en mars 2018. Les discussions qui se sont engagées à cette occasion en ont guidé le contenu et la conception. Les organisations suivantes ont participé à ces ateliers : Accenture, l'Institut américain de normalisation, Caribou Digital, le Centre pour le développement mondial, la *Digital Impact Alliance* (DIAL), Ernst & Young, la Commission européenne, l'Alliance FIDO, la Fondation Bill & Melinda Gates, le *Government Digital Service*, la GSMA, ID2020, l'OACI, l'IOM, iSPIRIT, Mastercard, Mercy Corp, Microsoft, l'Institut national des normes et de la technologie des États-Unis, Omidyar Network, *One World Identity*, l'*Open Identity Exchange*, l'*Open Society Foundation*, Plan International, PricewaterhouseCoopers, la *Secure Identity Alliance*, Simprints, le Forum économique mondial, le Programme des Nations Unies pour le développement, le HCR, l'UNICEF, USAID, *Vital Strategies* et WFP.

1. INTRODUCTION

Les systèmes d'identification fiables et inclusifs, tels qu'ils sont consacrés dans la cible 16.9 des Objectifs de développement durables (ODD), qui confie aux pays la charge de « garantir à tous une identité juridique, notamment grâce à l'enregistrement des naissances », sont essentiels au développement. Les individus doivent pouvoir faire la preuve de leur identité juridique pour avoir accès aux droits et aux services. Sans cette preuve, elles peuvent se retrouver exclues de la vie politique, économique et sociale. S'agissant des États, les systèmes d'identification modernes permettent une administration et une prestation des services plus efficaces et transparentes, une réduction de la fraude et des abus associés aux virements et aux paiements des prestations, une sécurité renforcée, une meilleure précision des statistiques essentielles à la planification et une plus grande capacité à répondre aux catastrophes et épidémies.

En dépit des avantages que procurent ces systèmes, on estime à environ 1 milliard le nombre de personnes qui ne disposent pas de preuve d'identité[1] dans le monde. Dans le but de combler ce « déficit d'identité », de nombreux pays ont commencé à réformer leurs systèmes d'identification existants et à mettre en place de nouveaux systèmes. À cet effet, la plupart ont misé sur les possibilités offertes par les nouvelles technologies d'identification numérique, notamment l'identification biométrique, les documents d'identité électroniques, comme les cartes intelligentes et les cartes d'identité mobiles, et les infrastructures d'authentification en ligne.

Ces avancées, en particulier conjuguées à d'autres technologies numériques notamment, telles que les systèmes de paiement mobiles et en ligne, ont le potentiel de combler les carences des systèmes d'identification papier. En parallèle, l'identification numérique pose de nombreux défis associés à la protection des données et de la vie privée, à la viabilité budgétaire et au choix à effectuer parmi les différentes technologies, ainsi qu'à la façon de les mettre en œuvre.

S'ils s'inscrivent dans une approche évolutive et interopérable, les systèmes d'identification numérique fiables sont sources d'économies pour les populations, les pouvoirs publics et les entreprises. À l'inverse, il est fort probable que les initiatives disparates et les investissements compartimentés dans les systèmes d'identification numérique feront double emploi, et ne pourront rivaliser avec les avantages considérables que les systèmes d'identification numérique universels sont capables d'apporter aux secteurs public et privé. Les approches communes et les systèmes d'identification fédérés au niveau régional ou sous-régional peuvent également aider à renforcer la proposition de valeur des systèmes d'identification numérique. La fiabilité et l'interopérabilité d'un système d'identification dépend de son degré de respect des normes techniques (ci-après les « normes »).

Les normes fixent des protocoles de communication, des régimes d'essai, des mesures de qualité et des meilleures pratiques cohérents et universellement partagés, concernant la saisie, le stockage, la transmission et l'utilisation des données d'identité, ainsi que le format et les caractéristiques des documents d'identité et des protocoles d'authentification. Elles sont dès lors cruciales à chaque stade du cycle de vie de l'identité, notamment l'inscription, la validation, la déduplication et l'authentification. Les normes aident à s'assurer que les composants des systèmes d'identité sont interopérables, peuvent être testés et sont capables d'atteindre les cibles de performance attendues. Sans normes, il est impossible de garantir l'efficacité d'un système d'identification interconnecté et interopérable.

[1] Estimation de la série de données ID4D de la Banque mondiale, 2018.

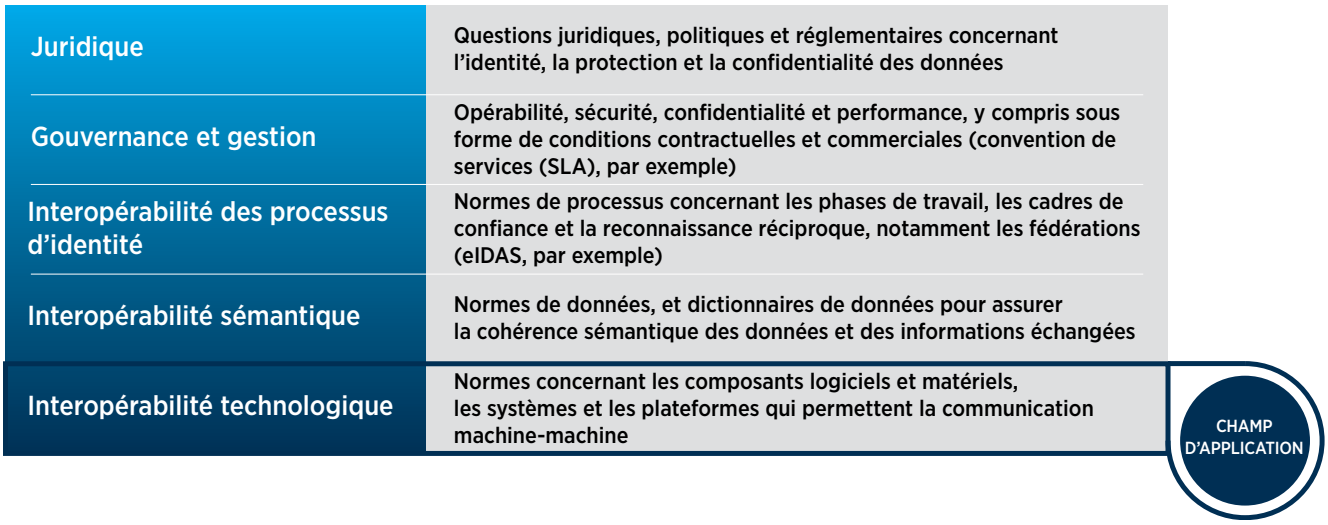
2. OBJECTIF

Les normes sont essentielles à la fiabilité, l'interopérabilité et la viabilité des systèmes d'identification. Le présent rapport se propose de recenser les normes et cadres techniques internationaux actuellement applicables d'un bout à l'autre du cycle de vie de l'identité en vue d'assurer l'interopérabilité technique des différents systèmes. Les acteurs de l'écosystème des systèmes d'identification peuvent utiliser ce catalogue de normes techniques comme source de référence. Une analyse du catalogue des normes existantes, organisées en catégories et sous-catégories, devrait aider à : i) identifier les domaines dans lesquels les normes font défaut ; ii) identifier les domaines dans lesquels l'existence de normes concurrentes amène à devoir faire des choix ; et iii) évaluer l'applicabilité des normes pour un pays en développement. Cette démarche devrait également faciliter l'échange d'expériences parmi les pays, et ainsi éviter à chaque pays ou acteur de « réinventer la roue ». Un arbre de décision des normes techniques, organisé par domaine technologique, est proposé pour faciliter la sélection des normes techniques dans le catalogue. Des études de cas par pays illustrent l'application de cet arbre de décision pour l'Estonie, l'Inde, le Malawi, le Pakistan et le Pérou.

3. CHAMP D'APPLICATION

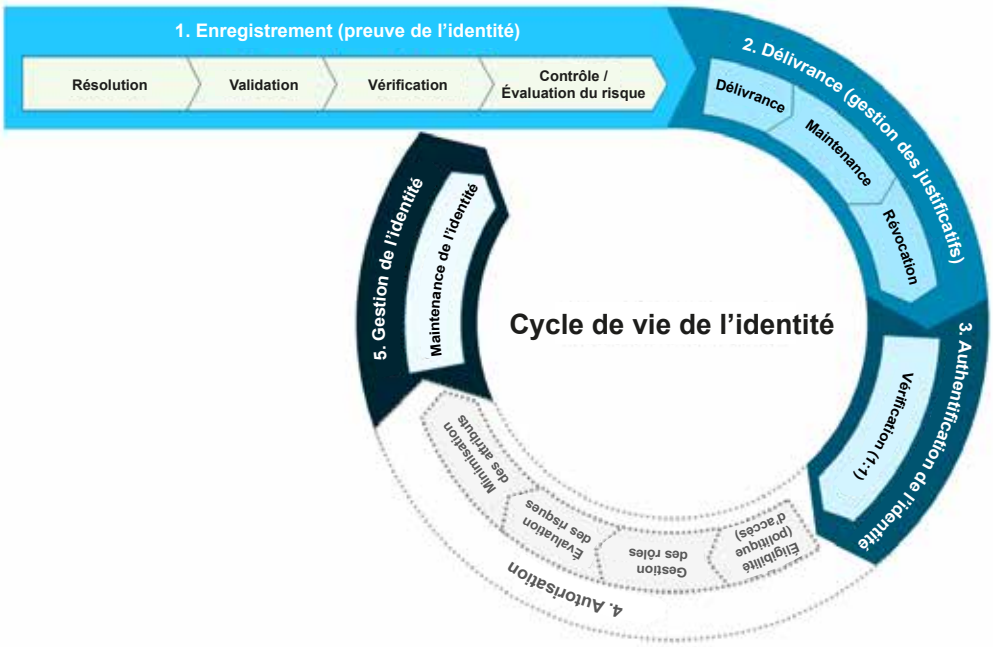
L'identité numérique est une notion générique, dont les acceptions diffèrent selon le contexte. Dans le présent document, l'identité numérique désigne un ensemble d'attributs et de justificatifs, saisis et stockés par des moyens électroniques et capables d'identifier une personne de façon unique. Les systèmes d'identité numérique peuvent prendre des formes diverses, chacune encadrée par des normes différentes. Cinq composantes forment le cadre d'interopérabilité pour les systèmes d'identification numérique (figure 1). Le présent rapport ne concerne que la composante « Interopérabilité technologique ». Les normes techniques qui relèvent du champ d'application du présent rapport sont les normes nécessaires à l'élaboration de systèmes d'identification numérique fiables et interopérables, qui permettent : i) la création d'une identité numérique pour chaque individu, après validation de son identité par des processus définis ; ii) la délivrance de justificatifs associés à son identité ; et iii) la mise en place de mécanismes permettant à chacun d'établir son identité (s'authentifier) au moyen de son identité numérique ou de ses justificatifs.

FIGURE 1 Cadre d'interopérabilité – Cinq composantes



4. CYCLE DE VIE DE L'IDENTITÉ

FIGURE 2 Cycle de vie de l'identité



Partout dans le monde, les écosystèmes de l'identité numérique, formés de modèles d'identité disparates et d'acteurs ayant des responsabilités, des intérêts et des priorités différents, sont de plus en plus complexes. Il est indispensable de comprendre les processus et les technologies mis en jeu dans l'identification numérique pour identifier les normes qui s'appliquent à un système donné. À cet effet, le présent chapitre offre un panorama du cycle de vie de l'identité numérique (basé sur le rapport *Technology Landscape for Digital Identification report* (2018)). Ce cadre sert ensuite à analyser les normes d'identification en question au chapitre 6.

Les identités numériques sont créées et utilisées dans le cadre d'un cycle de vie qui comporte trois stades fondamentaux : i) l'enregistrement (inscription et validation) ; ii) la délivrance des documents ou justificatifs ; et iii) la vérification de l'identité pour autoriser la prestation des services ou l'exécution des transactions. Les fournisseurs d'identité assurent en outre la gestion continue du système, notamment l'actualisation et la révocation ou la résiliation des identités ou des justificatifs (voir figure 2 ci-dessus).

4.1 Enregistrement

L'enregistrement est l'étape la plus importante de la création d'une identité numérique. Le processus se divise en deux phases consécutives : l'inscription et la validation.

4.1.1 Inscription

C'est au cours de la phase d'inscription que sont saisis et enregistrés les principaux attributs qui composent l'identité d'une personne qui déclare une certaine identité. Il peut s'agir de données biographiques (nom, date de naissance, sexe, adresse et adresse électronique, par exemple) ou biométriques (empreintes digitales et scan de l'iris, par exemple), ainsi que d'autres attributs, de plus en plus nombreux. Les attributs saisis pendant cette phase et la méthode utilisée ont des répercussions importantes sur la fiabilité de l'identité (voir plus bas les observations concernant les niveaux de garantie), ainsi que sur son utilité et son interopérabilité avec d'autres systèmes d'identité nationaux et internationaux.

4.1.2 Validation

Une fois que la personne a déclaré une identité pendant la phase d'inscription, cette identité est validée par comparaison des attributs présentés avec les données existantes. La phase de validation garantit que l'identité existe (le déclarant est vivant) et qu'une seule personne la déclare

(le déclarant est unique dans la base de données). Dans les systèmes d'identité numérique modernes, on vérifie le caractère unique d'une identité en procédant à un exercice de déduplication pour s´assurer que les attributs ne sont pas déjà utilisés et associés à une autre identité dans le système. Pour cela, on procède à une vérification 1 : N à partir des données biométriques. Il est également possible d'établir des liens entre l'identité déclarée et les identités présentes dans d'autres bases de données (par exemple, les registres d'état civil, registres de la population, etc.).

4.2 Délivrance

Avant qu'une personne puisse utiliser un justificatif pour faire valoir son identité, l'identité enregistrée est soumise à un processus de délivrance ou d'accréditation, à l'issue duquel les fournisseurs d'identité peuvent délivrer différents types de justificatifs (numéros d'identification, cartes intelligentes et certificats, par exemple). Pour considérer qu'une identification est numérique, les justificatifs délivrés doivent être électroniques, autrement dit qu'ils doivent stocker et communiquer les données de façon électronique.

Types de systèmes de justificatifs électroniques :

- **Cartes intelligentes :** ces cartes intègrent des éléments de sécurité avancés, et contiennent une puce informatique sur laquelle sont enregistrées une clé cryptographique numérique et/ou des données biométriques. Les cartes intelligentes peuvent se présenter sous la forme d'une carte avec ou sans contact ou d'une carte SIM avec fonction NFC (communication en champ proche). Les données stockées sur une carte intelligente peuvent être consultées hors ligne, de manière à permettre de vérifier l'identité en l'absence de connexion Internet ou de réseau mobile.
- **Cartes avec code à barres 2D :** ces cartes peuvent être personnalisées au moyen d'un code à barres 2D chiffré, contenant les données personnelles et biométriques d'une personne. Ce code à barres vient, soit remplacer, soit compléter, une puce informatique. Le code à barres 2D est un moyen économique de fournir une identité numérique et de vérifier l'identité du porteur de la carte en comparant les caractéristiques biométriques du porteur à celles contenues dans la carte. L'Afrique (Mali et Ghana notamment), l'Amérique latine et le Moyen-Orient (Liban notamment) ont déployé ce système à grande échelle. Plus récemment, l'Égypte l'a utilisé pour vérifier l'identité des votants lors des dernières élections.
- **Identité mobile :** il est possible d'utiliser les téléphones et autres dispositifs mobiles pour offrir aux individus une identité numérique portable et un moyen d'authentification permettant d'exécuter une diversité de transactions en ligne. Les fournisseurs peuvent, par exemple, délivrer des cartes SIM comportant des certificats numériques. Ils peuvent aussi utiliser d'autres équipements de réseaux mobiles qui permettent de vérifier simplement et en toute sécurité l'identité des utilisateurs des services administratifs en ligne *(eGovernment)* et autres plateformes publiques ou privées.
- **Identité (justificatif) dans un entrepôt centralisé ou dans le nuage :** contrairement aux systèmes qui délivrent des justificatifs portables, cartes intelligentes et cartes SIM notamment, certains systèmes se contentent de stocker les certificats et les données biométriques sur un serveur. Ce type de système ne permet pas la délivrance d'un dispositif physique pour le stockage des justificatifs. Le numéro d'identité peut être délivré sous une forme non électronique (en Inde, par exemple, le programme Aadhaar ne délivre qu'un reçu papier). Un environnement anti-fraude avec génération et gestion de clés cryptographiques pour protéger contre le vol les justificatifs d'identité stockés dans l'entrepôt centralisé permettra de renforcer le niveau de sécurité et de garantie du système d'identité.

4.3 Authentification

Une fois enregistrée, et après réception de ses justificatifs, une personne peut utiliser son identité numérique pour accéder aux bénéfices et services associés. Par exemple, les contribuables peuvent payer leurs impôts au moyen d'un portail de services publics en ligne, tandis que les clients des banques peuvent utiliser leurs cartes de paiement intelligentes ou leur application de banque en ligne ou mobile pour réaliser des transactions. Pour accéder aux services, l'utilisateur doit s'authentifier au moyen d'un ou plusieurs facteurs qui relèvent le plus souvent de l'une des trois catégories suivantes : quelque chose que l'on connaît, quelque chose que l'on a ou quelque chose que l'on est. L'authentification au moyen de ces attributs peut être réalisée au travers de différents mécanismes :

- **Cartes intelligentes :** les possesseurs de carte intelligente peuvent prouver leur identité (s'authentifier) au moyen d'un ou plusieurs facteurs d'authentification, lesquels offrent des niveaux de garantie variables. Par exemple, un simple code PIN pour les opérations présentant un risque faible, ou une signature numérique reposant sur la technologie d'infrastructure à clés publiques (PKI) pour les utilisations à risque fort. Les empreintes digitales sont un moyen d'établir avec certitude un lien avec l'utilisateur. Les cartes intelligentes, dotées d'une puce électronique sur laquelle sont stockées les données d'identité, permettent à leur détenteur de s'en servir afin de s'authentifier hors ligne ou dans les régions isolées disposant d'une connectivité limitée, sans consultation d'une base d´identité centrale. En effet, la puce permet de réaliser, en local, une procédure

d´authentification, en comparant les données biométriques (empreintes digitales par exemple) du détenteur de la carte avec les données stockées sur la puce (Match on Card).

- **Identité mobile :** l'identité mobile utilise les applications sur smartphones, l'authentification par protocole USSD ou par SMS ou les cartes SIM, et peut incorporer plusieurs facteurs d'authentification offrant des niveaux de garantie variables. Par exemple, un simple code PIN pour les opérations présentant un risque faible ou bien, pour les transactions présentant un risque fort, des solutions d'authentification à facteurs multiples (avec recours à la biométrie notamment) ou une signature mobile numérique reposant sur la technologie d'infrastructure à clés publiques (PKI) comportant un élément sécurisé. Il est possible de renforcer l'authentification au moyen d'un troisième et d'un quatrième facteurs, comme le lieu où se trouve l'individu ou l'analyse dynamique de ses gestes (façon de réaliser sa signature, par exemple).
- **Identité dans un entrepôt centralisé ou dans le nuage :** au lieu de délivrer un document d'identité ou un justificatif mobile, un système d'identité numérique peut faire appel à la biométrie pour l'authentification à distance. Dans ce cas, l'identité est évaluée et vérifiée au moyen d'un ordinateur ou d'un autre dispositif doté d'un lecteur biométrique connecté au nuage. Un système basé dans le nuage élimine le besoin de justificatifs physiques et le coût qui y est associé, mais nécessite une infrastructure TIC fiable pour assurer la connectivité, la sécurité de la base de données centralisée dans un entrepôt (ou plusieurs entrepôts pour les infrastructures TIC les plus robustes) et la protection des données transmises entre le dispositif biométrique et la base centrale lors du processus d´authentification (confidentialité et intégrité des données).

4.4 Gestion du cycle de vie

Pendant tout le cycle de vie, les fournisseurs d'identité numérique gèrent et organisent le système d'identité, notamment les installations, le personnel, la tenue des registres, la conformité, l'audit et l'actualisation du statut et du contenu des identités numériques. En effet, les utilisateurs (les détenteurs d'identité) pourront être amenés à devoir actualiser un ou plusieurs attributs liés leur identité, par exemple leur adresse, leur situation maritale, leur profession, etc. De leur côté, les fournisseurs d'identité pourront devoir révoquer une identité, autrement dit annuler l'identité numérique pour des questions de fraude ou de sécurité par exemple, ou résilier une identité dans le cas du décès de l'individu.

4.5 Fédération

La fédération est la capacité d'une organisation d'accepter l'identité générée et gérée par une autre organisation, et repose sur la confiance entre ces deux organisations. L'organisation utilisatrice doit avoir la conviction que l'organisation de confiance dispose de politiques et de normes comparables aux siennes, et qu'elle les applique. Les protocoles de fédération et le cadre d'assurance facilitent la fédération de l'identité numérique dans et entre les organisations et les pays. Le fournisseur du justificatif utilise des protocoles de fédération tels que SAML (*Security Assertion Mark-up Language*) pour transmettre le résultat de l'authentification à l'organisation utilisatrice. Cette dernière saisit le justificatif et l'envoie à l'organisme émetteur pour vérification. Après vérification du justificatif, l'organisme émetteur envoie un ensemble d'informations sur l'utilisateur, le résultat de l'authentification et le degré de fiabilité des justificatifs utilisés pour authentifier l'utilisateur. Pour une utilisation efficace de la fédération partout dans le monde, l'accord et l'alignement avec le cadre d'assurance défini par l'ISO et l'adoption de protocoles de fédération en tant que normes sont essentiels.

La fédération peut intervenir à des niveaux multiples :

- Un organisme peut accepter les justificatifs émis par un autre organisme, tout en authentifiant et autorisant l'individu localement :
  - Un passeport émis par le Département d'État des États-Unis est accepté comme justificatif valable par un pays étranger ; pour autant, les services de l'immigration de ce pays authentifient le titulaire et exigent un visa (autorisation).
- Un organisme peut accepter les caractéristiques spécifiques (attributs) décrivant un individu qui émanent d'un autre organisme :
  - Votre banque vous demandera votre notation de crédit délivrée par l'un des organismes de notation du crédit, plutôt que de détenir et d'actualiser elle-même ces informations.
- Un organisme peut accepter une décision d'autorisation prise par un autre organisme :
  - Aux États-Unis, par exemple, un permis de conduire vous autorisant à conduire dans un État est accepté dans un autre.

Le cycle de vie de l'identité exige l'application de normes techniques à chaque étape et sous-étape (voir Chapitre 6). Dans une large mesure, les types d'attributs (biométriques, biographiques et autres) saisis pendant l'inscription et les méthodes utilisées pour les enregistrer ont des répercussions importantes sur le degré de fiabilité et de confiance que le système d'identité est capable d'offrir, ainsi que sur son utilité et son interopérabilité avec d'autres systèmes d'identité nationaux et internationaux.

5. NORMES TECHNIQUES RELATIVES À L'IDENTITÉ NUMÉRIQUE

5.1 En quoi les normes sont-elles importantes ?

En règle générale, les normes techniques établissent le cahier des charges et les procédures concernant le fonctionnement, l'entretien et la fiabilité des matériaux, matériels, produits, méthodes, procédés et services dont se servent les individus ou les organisations. Les normes garantissent la mise en œuvre de protocoles universellement reconnus, nécessaires pour assurer le fonctionnement, la performance, la compatibilité et l'interopérabilité. Ces facteurs sont à leur tour indispensables à la mise au point et à l'adoption d'un produit. Si l'adoption de normes influe favorablement sur la pénétration du marché et sur le commerce international, leur absence risque de compromettre l'efficacité et la fiabilité d'un système d'identité, en matière d'interopérabilité, de connectivité et de dépendance à un fournisseur unique notamment.

Alors que les cartes d'identité électroniques remplacent progressivement les systèmes papier, l'interopérabilité entre les différents systèmes, technologies et dispositifs, ainsi que les impératifs de sécurité sur lesquels reposent ces systèmes, sont de plus en plus complexes. Il devient dès lors d'autant plus important de disposer de normes pour encadrer la gestion de l'identité, et de savoir choisir parmi les différentes normes proposées. Cependant, la rapidité des innovations, les bouleversements technologiques, la diversification des solutions techniques, l'évolution des impératifs d´interopérabilité et de connectivité, et la nécessité d´améliorer en permanence la mise en œuvre des normes ne facilitent en rien la tâche.

5.2 Organismes de normalisation

Les normes sont définies de façon rigoureuse par des organismes créés et mandatés expressément à cet effet. Dans le cas des normes qui encadrent les technologies de l'information et des communications (les TIC), ces organismes, avec l'appui d'experts, fixent, surveillent et actualisent en continu les normes techniques destinées à satisfaire des besoins variés. Sans pour autant s´y limiter, ces organismes se concentrent sur la production de normes liées aux divers protocoles qui facilitent la fonctionnalité et la compatibilité des solutions techniques et garantissent ainsi l´interopérabilité entre les systèmes. Ces normes, et les mises à jour qui s'y rapportent, sont régulièrement publiées à l'intention du public[2].

Selon la veille technologique de l'Union internationale des télécommunications (UIT), plusieurs organismes s'emploient à élaborer des normes techniques pour les systèmes d'identification numérique. Il s'agit d'organisations internationales, comme les agences spécialisées des Nations Unies, de consortiums d'entreprises et d'organismes nationaux. Chacun de ces trois types d'organismes est brièvement décrit ci-dessous.

- **Organisations internationales.** De grandes organisations internationales prennent une part active à l'élaboration de normes techniques utiles à l'identité numérique : l'Organisation internationale de normalisation (ISO), la Commission électrotechnique internationale (CEI), le Secteur de la normalisation des télécommunications de l'UIT (UIT-T), l'Organisation de l'aviation civile internationale (OACI), l'Organisation internationale du travail (OIT), le Comité européen de normalisation (CEN), le *World Wide Web Consortium* (W3C) et l'I*nternet Engineering Task Force* (IETF) / *Internet Society*.
- **Organismes nationaux.** Outre les organisations internationales, des organismes nationaux élaborent eux aussi des normes techniques, reposant sur leurs besoins et systèmes propres. Parmi ces organismes, on peut notamment citer notamment l'Institut américain de normalisation (ANSI), l'Institut national des normes et de la technologie (NIST) des États-Unis, le Comité international pour les normes relatives aux technologies de l'information (INCITS), basé aux États-Unis, le ministère de la Sécurité intérieure (*Department of Homeland Security* – DHS) des États-Unis, le ministère de la Défense (*Department of Defense* – DoD) des États-Unis, *Standards Australia* (SA), l'Institut de normalisation suédois (SIS), l'Association nationale suédoise de biométrie (SNBA), l'Institut de normalisation allemand (DIN), l'Association française de normalisation (AFNOR), l'Organisme de normalisation néerlandais (NEN), l'Autorité indienne de l'identification unique (UIDAI), le Bureau indien de normalisation (BIS) et l'Organisme pakistanais de normalisation (PSA).
- **Consortiums d'entreprises.** Des consortiums d'entreprises et quelques organisations à but non lucratif participent également, soit à l'élaboration des normes, soit à la promotion de bonnes pratiques visant à satisfaire les besoins de leurs membres. Principaux exemples : le *Biometric Consortium*, consortium parrainé par le gouvernement des États-Unis, la *Secure Identity Alliance* (SIA), le *Center*

[2] FAQ de l'IEEE (lien)

for Identification Technology Research (CITeR), le *Biometrics Council* de l'IEEE, le *Biometrics Institute* (Australie), la *Smart Card Alliance*, l'*International Biometrics and Identification Association* (IBIA), l'initiative Kantara, *Open Identity Exchange*, *Open Security Exchange*, l'*Asian Pacific Smart Card Association* (APSCA), l'*Organization for the Advancement of Structural Information of Standards* (OASIS), la *Fast IDentity Online* (FIDO) *Alliance* et l'*Open ID Foundation*.

Si on observe les grands organismes de normalisation, on constate que les pays et les consortiums d'entreprises les plus actifs (par l'entremise des sous-comités et groupes de travail, par exemple) sont en contact et collaborent avec l'Organisation internationale de normalisation, ou ISO, pour modifier ou confirmer les normes qui concernent leurs besoins. Voir l'Annexe A pour en savoir plus sur les comités, sous-comités et groupes de travail techniques de l'ISO qui travaillent sur les normes concernant le cycle de vie de l'identité numérique.

5.3 Normes techniques

La présente rubrique énumère les normes techniques recensées pour les systèmes d'identité. Elles concernent pour la plupart le justificatif utilisé pour authentifier l'utilisateur. Le présent rapport ne contient et ne décrit pas les normes techniques qui concernent les applications d'identité partagées avec une application logicielle (application web / ordinateur de bureau / portail). Les normes techniques sont regroupées en deux tableaux. Le premier tableau dresse la liste des normes nécessaires pour assurer l'interopérabilité. Le second dresse la liste des normes qui concernent la fiabilité des systèmes d'identification et énoncent diverses contraintes, en matière de sécurité et de qualité notamment. Ces normes sont réexaminées en continu par les organismes de normalisation. Dans les deux tableaux, les normes sont accompagnées d'un lien dirigeant vers un site Internet contenant des informations à propos de la norme en question. La page du site de l'ISO énumérant les différentes normes donne des informations sur la version la plus récente de la norme en question, si elle est disponible, et contient un lien dirigeant vers cette version.

Normes techniques pour assurer l'interopérabilité

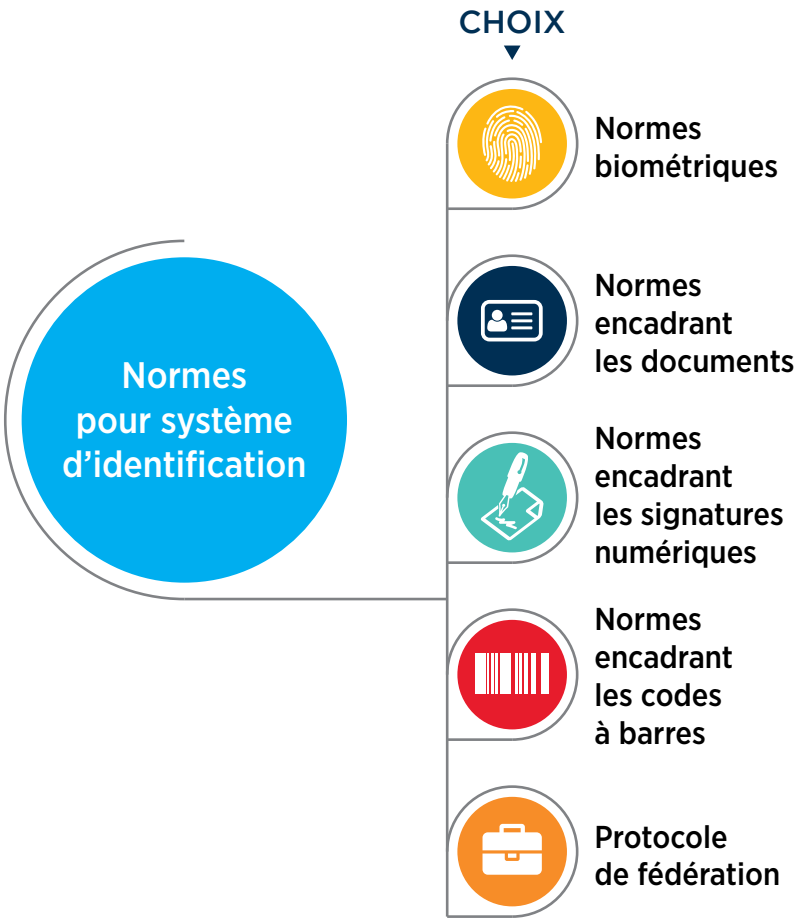
Les normes relatives à l'interopérabilité relèvent des six grands domaines ci-dessous :

1. Biométrie – Norme d'image. Plusieurs normes concurrentes sont utilisées pour prendre une image du visage (PNG, JPEG, JPEG2000 dans la plupart des systèmes, et éventuellement GIF/TIFF (normes propriétaires) dans quelques-uns). L'image des empreintes digitales a recours aux normes JPEG, JPEG2000 et WSQ. L'image des empreintes digitales a recours aux normes JPEG, JPEG2000 et WSQ. Des notes sont proposées pour guider le choix de la norme d'image, notamment pour les images du visage ou des empreintes digitales.
2. Biométrie – Pour assurer la reconnaissance biométrique dans un environnement à systèmes ouverts (au sens où le système va interagir avec d´autres systèmes externes ou où le système utilise des application open source), il est indispensable d'appliquer des normes qui encadrent les formats d'échange de données biométriques et d'autres qui encadrent les interfaces biométriques si l'on veut garantir un échange complet, qui atteste de l´intégralité et de l´intégrité des données transmises, et une interopérabilité optimale. Les données biométriques conformes à un format d'échange de données biométriques certifié ISO 19794 représentent la composante essentielle de l'interopérabilité biométrique. Les normes qui encadrent les formats d'échange de données biométriques définissent des formats différents selon les modalités biométriques utilisées. Les parties qui s'entendent sur un format d'échange de données biométriques certifié ISO 19794 devraient pouvoir décoder leurs données biométriques mutuelles sans difficulté. Les normes applicables à l'interface biométrique sont les normes ISO 19785 – Technologies de l'information – Cadre de formats d'échange biométriques communs et ISO 19784 – Technologies de l'information – Interface de programmation d'applications biométriques (BioAPI). Ces normes facilitent l'échange de données biométriques au sein d'un même système ou parmi plusieurs systèmes. La norme ISO 19785 définit la structure de base d'un registre d'informations biométriques (BIR) normalisé, qui comporte le registre dans lequel est consigné l'échange de données biométriques, avec des métadonnées comme la date de saisie, la date d'expiration, la présence de chiffrement ou non, etc. La norme 19784 définit une API système ouverte, qui facilite les communications entre les applications logicielles et les services de technologie biométrique sous-jacents.
3. Carte / Carte intelligente – Pour les pays qui délivrent un justificatif tangible, carte d'identité électronique physique, par exemple, les normes comme ISO 7810 sont utiles pour assurer l'interopérabilité et l'interconnectivité. Pour les cartes avec contacts sur lesquelles est insérée une puce informatique en relief,

la norme ISO / IEC 7819 s'applique partout dans le monde. Pour les cartes sans contact, lorsque la puce informatique est incorporée à l'intérieur de la carte, c'est la norme ISO / IEC 14443 qui est suivie. Pour les cartes qui peuvent également servir de documents de voyage électroniques, incluant les cartes d´identité, les passeports, les permis de conduire électroniques et les autres documents de voyage lisibles à la machine (MRTD) utilisés pour franchir les frontières, la conformité à la norme OACI 9303 est préconisée. Chaque système d'identité sélectionnera un type de carte en fonction de critères variés, comme le coût ou les éléments de sécurité.

4. Signatures numériques – Plusieurs normes non concurrentes sont indiquées. Elles s'appliquent en fonction de l'utilisation de la signature numérique pour les systèmes d'identité.
5. Code à barres 2D – La colonne contenant les notes d'aide au choix de la norme présente les avantages et les inconvénients des deux formats de codes à barres à deux dimensions couramment utilisés dans les systèmes d'identité, le PDF417 et le code QR.
6. Protocoles de fédération – On a de plus en plus recours à l'association *Open ID Connect* et OAuth pour répondre aux besoins de fédération, alors que le protocole SAML a été beaucoup utilisé précédemment.

FIGURE 3 Normes pour système d'identification



La liste des normes applicables pour un système d'identité va consister en la somme des normes retenues dans chacune des six catégories ci-dessus.

La figure 4 présente un schéma d'arbre de décision, qui permet de sélectionner les normes applicables en fonction des technologies retenues pour la mise en œuvre du système d'identification.

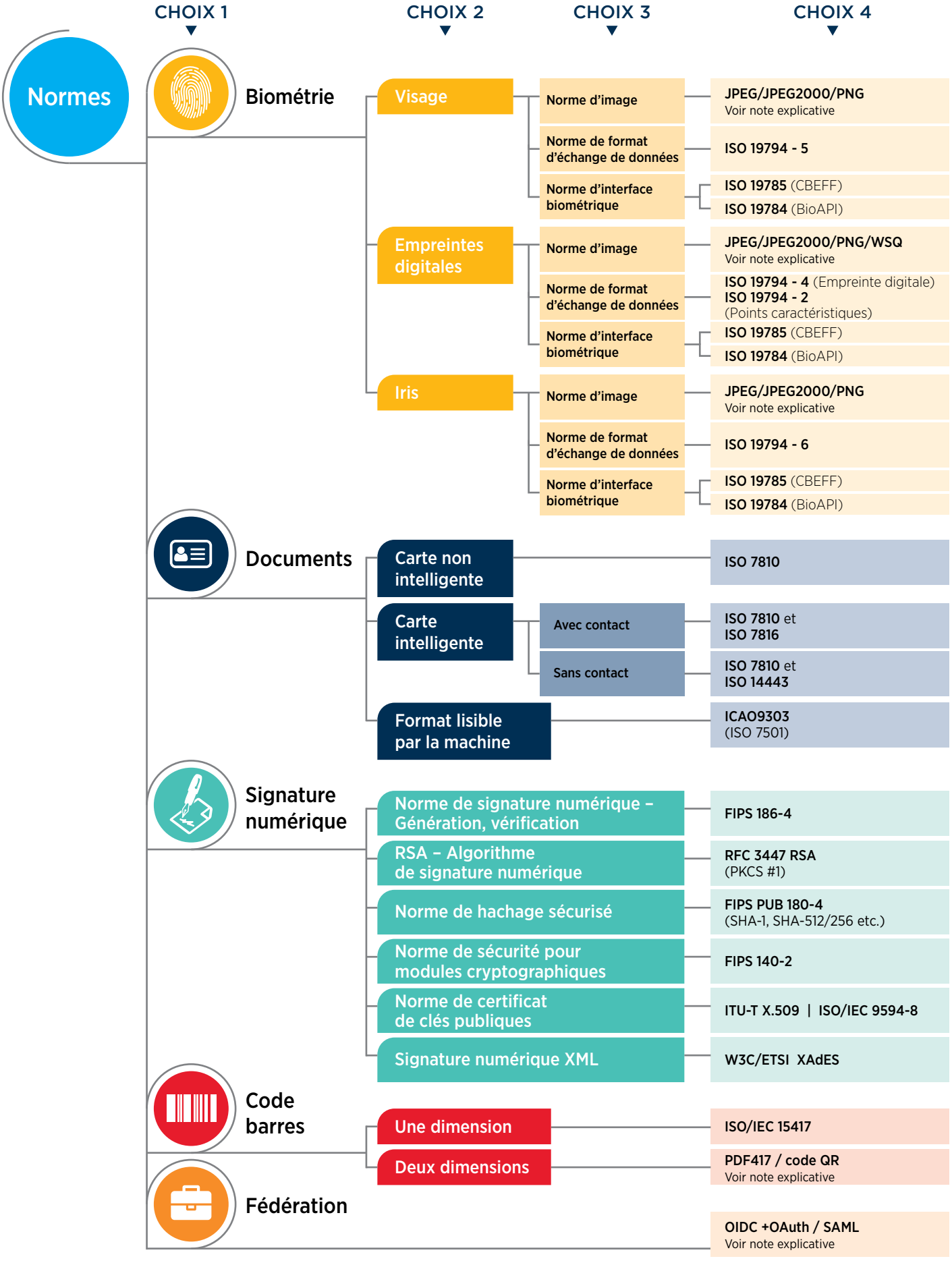
1. Partir du sommet et descendre le long de l'arbre en suivant chaque branche tant que la catégorie de technologies ou de normes mentionnée à chaque embranchement s'applique au système d'identité.
2. Les normes citées à l'extrémité de la branche de l'arbre sont les normes applicables en fonction des décisions prises en matière de choix de technologie et de conception système.
3. À certains embranchements, il faudra choisir parmi plusieurs normes concurrentes. Le tableau contient des notes d'aide au choix qui aideront à sélectionner l'une des normes concurrentes disponibles.
4. Le tableau dressant la liste des normes contient une brève description des normes et un lien renvoyant à celles-ci.

Normes techniques pour des systèmes d'identité fiables

Le tableau « Normes techniques pour des systèmes d'identité fiables » énumère les normes qui contiennent des lignes directrices concernant les aspects des systèmes d'identification liés à la qualité, aux méthodes d'essai, à la confidentialité des données et à l'accessibilité, en vue de renforcer la fiabilité de ces systèmes. Elles donnent aux responsables de la mise en œuvre des systèmes d'identification les moyens d'adopter des lignes directrices et des bonnes pratiques en terme de normes pour leurs systèmes. Dans le cadre de son système Aadhaar, l'Inde a par exemple publié un document définissant des lignes directrices en matière de sécurité encadrant le recours à la

FIGURE 4

ARBRE DE DÉCISION CONCERNANT LE CHOIX DES NORMES



N°	Domaine d'interopérabilité	Sous-domaine	Norme / spécification (nom commun)	Description de la norme	Organisme de normalisation	Note d'aide au choix de la norme
A.1	Biométrie	Norme d'image	ISO/IEC 15444-1 (JPEG2000)	Norme d'encodage d'images (compression avec ou sans perte de qualité)	ISO et IEC	Le format PNG est un format d'images sans perte de qualité peu utilisé par les systèmes d'identification. La plupart des systèmes ont retenu les formats JPEG et JPEG2000 pour les photographies. L'Inde utilise le format JPEG2000, considéré plus ouvert que le format JPEG. La norme OACI 9303 autorise à la fois le format JPEG et le format JPEG2000. Le format JPEG2000 est recommandé pour les passeports de l'Union européenne, car il donne lieu à des fichiers plus légers que les images compressées au format JPEG. La norme WSQ est traditionnellement utilisée pour les images d'empreintes digitales. De nombreux systèmes d'identification y ont recours. Le système d'identification indien utilise le format JPEG2000 pour les images des empreintes digitales et de l'iris. Aux États-Unis, la plupart des forces de l'ordre utilisent le format WSQ pour un stockage efficace des images d'empreintes digitales compressées à 500 ppi. Pour les empreintes digitales compressées à 1 000 ppi, les forces de l'ordre (dont le FBI) privilégient le format JPEG2000 au format WSQ.
A.2	Biométrie	Norme d'image	ISO/IEC 15948, (PNG)	Technologie – Infographie et traitement d'images – Portable Network Graphics – Compression sans perte de qualité	W3C	
A.3	Biométrie	Norme d'image	ISO/IEC 10918:1994 JPEG	Norme d'encodage d'images – Compression avec perte de qualité	ISO et IEC	
A.4	Biométrie	Norme d'image	WSQ	Algorithme de compression utilisé pour les images d'empreintes digitales en niveaux de gris	NIST	
B.1	Biométrie	Échange de données – Visage	ISO/IEC 19794-5:2011 (Image du visage)	Formats d'échange de données d'image du visage biométriques. La norme définit les contraintes de prise de vue, de qualité photographique, de numérisation et de format applicables aux images du visage à utiliser dans le cadre, tant de la vérification humaine que de la reconnaissance automatisée par ordinateur.	ISO et IEC	
B.2	Biométrie	Échange de données – Empreintes digitales	ISO/IEC 19794-4:2011 (Empreintes digitales)	Format d'échange de registres de données pour stocker, enregistrer et transmettre les informations issues d'un ou plusieurs domaines d'images digitales ou palmaires pour échange ou comparaison.	ISO et IEC	
B.3	Biométrie	Échange de données – Iris	ISO/IEC 19794-6:2011 (Iris)	Formats d'échange de l'image de l'iris pour système biométrique d'inscription, de vérification et d'identification.	ISO et IEC	
B.4	Biométrie	Échange de données – Points caractéristiques de référence	ISO/IEC 19794-2:2011 (Points caractéristiques de référence)	Trois formats de données pour la représentation des empreintes digitales, ayant recours à la notion fondamentale des points caractéristiques de référence (*minutiae*) pour l'échange et le stockage de ces données : i) format basé sur des registres ; ii) format ordinaire ; et iii) format compact pour utilisation sur carte intelligente dans une application « Match-on-Card ».	ISO et IEC	
B.5	Biométrie	Échange de données – Signature	ISO/IEC 19794-7:2014 (Signature)	Formats d'échange de données pour données de signature / analyse dynamique de la signature (analyse comportementale), captées sous la forme d'une série temporelle multidimensionnelle au moyen de dispositifs, comme les tablettes de numérisation ou les systèmes à stylet perfectionnés.	ISO et IEC	

(suite)

N°	Domaine d'interopérabilité	Sous-domaine	Norme / spécification (nom commun)	Description de la norme	Organisme de normalisation	Note d'aide au choix de la norme
B.6	Biométrie	Norme d'interface biométrique	ISO 19785 :2015 *Common Biometric Exchange Format Framework* – CBEFF (ou cadre de formats d'échange biométriques communs)	Les normes d'interface biométrique comprennent les normes ISO/IEC 19785 et ISO/IEC 19784 (BioAPI). Ces normes concernent l'échange de données biométriques au sein d'un système ou parmi plusieurs systèmes. ISO/IEC 19785 définit la structure de base d'un Registre d'informations biométriques (*Biometric Information Record* – BIR) normalisé, qui comporte le registre dans lequel est consigné l'échange de données biométriques, avec des métadonnées comme la date de saisie, la date d'expiration, la présence de chiffrement ou non, etc.	ISO/IEC	
B.7	Biométrie	Norme d'interface biométrique	ISO/IEC 19784-1:2018 (spécification BioAPI)	Définit une API système ouverte qui autorise les communications entre les applications logicielles et les services technologiques biométriques sous-jacents.	ISO/IEC	Certaines organisations (l'Union européenne, Interpol et les États-Unis, par exemple) ont retenu le format de base d'échange d'images d'empreintes digitales et autres images ANSI/NIST-ITL.
C.1	Carte		ISO/IEC 7810	Cartes d'identification – Caractéristiques physiques	ISO et IEC	
C.2	Carte intelligente		ISO/IEC 7816	Cartes d'identité électroniques (e-ID) / Cartes intelligentes – Normes pour cartes avec contacts	ISO et IEC	
C.3	Carte intelligente		ISO/IEC 14443	Cartes d'identité électroniques (e-ID) / Cartes intelligentes – Normes pour cartes sans contact	ISO et IEC	
C.4	Carte intelligente		ICAO 9303 adoptée en tant qu'ISO/IEC 7501	Norme pour documents de voyage à lecture automatique	ICAO ISO et IEC	
C.5	Carte intelligente		ISO/IEC 24727	Ensemble d'interfaces de programmation pour interactions entre les cartes à circuit intégré et les applications externes	ISO et IEC	

(suite)

N°	Domaine d'interopérabilité	Sous-domaine	Norme / spécification (nom commun)	Description de la norme	Organisme de normalisation	Note d'aide au choix de la norme
D.1	Code barres	1D (une dimension)	ISO/IEC 15417 :2012	Techniques automatiques d'identification et de capture des données – Spécifications applicables à la symbologie de code barres 128.	ISO/IEC	Les codes 1D représentent les données horizontalement au moyen du format barres noires et espaces blancs. Ils conviennent aux nombres courts, mais au-delà de 25-30 caractères, ils peuvent devenir très longs. L'encodage du texte et des URL est impossible. Les codes barres 2D peuvent stocker plus de mille caractères, y compris les URL et les images. Le PDF147 est un code barres empilé lisible au moyen d'un scanner linéaire simple. Il comporte des capacités de correction d'erreurs intégrées au sein de ses rangées linéaires haute résolution, de sorte que la dégradation de ce type de code barres ne pose pas un problème majeur. Il se présente sous la forme d'un rectangle allongé, et est très couramment employé dans les cartes d'identification. Ce format nécessite une résolution beaucoup plus importante, que ce soit pour imprimer les codes barres ou pour les afficher sur un dispositif. Le code QR est formé de grands carrés. S'il prend plus de place que le petit PDF147 rectangulaire, il offre cependant une capacité de 3 à 4 fois supérieure. La création des codes QR est également plus simple que celle des codes barres PDF147. Les codes QR n'utilisent pas de scanners linéaires, mais des capteurs d'image. La résolution est dès lors importante, mais pas dans la même mesure qu'avec les codes barres PDF147. Les applications mobiles simples peuvent facilement scanner les codes QR. Il est en revanche plus difficile de scanner les codes à barre PDF147, d'où la nécessité de disposer d'un matériel onéreux uniquement pour scanner ces codes. Pour l'authentification hors ligne, l'Inde a recours à un code QR qui intègre des données chiffrées à signature numérique. Certains pays de la Communauté d'Afrique de l'Est utilisent une norme PDF147 pour le code barres figurant sur leurs cartes d'identité.
D.2	Code barres	2D (deux dimensions)	ISO/IEC 18004:2015—Code QR (ou code à réponse rapide)	Caractéristiques de la symbologie de code QR, méthodes de codage des caractères de données, formats de symboles, caractéristiques dimensionnelles, règles de correction d'erreurs, algorithme de décodage de référence, exigences de qualité de production et paramètres d'application sélectionnables par l'utilisateur.	ISO et IEC	
D.3	Code barres	2D (deux dimensions)	ISO/IEC 15438: 2015—PDF417	Exigences applicables aux caractéristiques de la symbologie de code barres, codage des caractères de données, formats de symboles, dimensions, règles de correction d'erreurs, algorithme de décodage de référence et nombreux paramètres d'application.	ISO et IEC	
E.1	Signatures numériques / cryptographie	Norme de signature numérique	FIPS 186-4 DSS	Cette norme définit les méthodes de génération de signatures numériques, pouvant servir à protéger les données binaires (couramment dénommées un message) et à vérifier et valider ces signatures numériques.	NIST	
E.2	Signatures numériques / cryptographie	Algorithme de signature numérique	RFC 3447 RSA (PKCS #1)	Utilisation de l'algorithme RSA pour génération et vérification des signatures numériques.	IETF Internet Society	
E.3	Signatures numériques / cryptographie	Norme de hachage sécurisé	SHS (FIPS PUB 180-4)	Cette norme définit les algorithmes de hachage sécurisés SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 et SHA-512/256.	NIST	

(suite)

N°	Domaine d'interopérabilité	Sous-domaine	Norme / spécification (nom commun)	Description de la norme	Organisme de normalisation	Note d'aide au choix de la norme
E.4	Signatures numériques / cryptographie	Sécurité	FIPS 140-2	Exigences de sécurité pour modules cryptographiques.	NIST	
E.5	Signatures numériques / cryptographie	Infrastructure à clés publiques	ITU-T X.509 | ISO/IEC 9594-8	Le cadre de certificats de clé publique défini dans cette Recommandation | Norme internationale définit les objets d'informations et les types de données d'une infrastructure à clés publiques (PKI), notamment les certificats de clé publique, les listes de révocation de certificats (CRL), le protocole d'accès à un courtier de confiance et les listes d'autorisation de validation (AVL).	UIT-T, ISO et IEC	
E.6	Signatures numériques / cryptographie	Signatures électroniques avancées XML	XAdES W3C	Tandis que XML-DSig est un protocole général pour la signature numérique des documents, XAdES définit des profils précis de XML-DSig, mettant ce protocole en conformité avec la réglementation européenne eIDAS.	W3C	
F.1	Fédération	Protocole	SAML v2—2005	La norme *Security Assertion Markup Language* (SAML) définit un protocole XML pour l'échange d'informations liées à la sécurité (authentification, autorisations et attributs, par exemple) entre des entités informatiques. SAML facilite l'interopérabilité entre des systèmes de sécurité disparates, et définit le protocole permettant d'exécuter des transactions en ligne sécurisées et capables de s'affranchir des frontières des sociétés.	OASIS	La norme SAML a été conçue uniquement pour les applications Internet, tandis qu'*OpenID Connect*, outre ces applications, prend également en charge les applications natives et les applications mobiles. *OpenID Connect* est plus récente et s'appuie sur le flux de processus OAuth 2.0. Testée et éprouvée, elle est le plus souvent utilisée par les sites d'achat en ligne, les applications Internet et les applications mobiles. Mobile Connect et les solutions de gestion de l'identité de Microsoft utilisent ce protocole. Les entreprises utilisent généralement la norme SAML, sa cousine aînée. Elle permet par exemple de se connecter en une seule fois à plusieurs applications dans une entreprise au moyen de son identifiant *Active Directory*. Le protocole EIDAS est basé sur SAML. Capable de prendre en charge à la fois les applications natives et les applications mobiles, outre les applications Internet, *OpenID Connect* est de plus en plus utilisée dans les nouvelles implémentations.
F.2	Fédération	Protocole	RFC 6749/ OAUTH 2	OAuth 2.0 est le protocole d'autorisation standard du secteur professionnel. Il fournit des flux d'autorisation spécifiques pour les applications Internet, les applications PC, les téléphones mobiles et les dispositifs de salon.	IETF	
F.3	Fédération	Protocole	Open ID connect	OpenID Connect 1.0 est une simple surcouche d'identification au protocole OAuth 2.0. Elle permet aux clients de vérifier l'identité de l'utilisateur final sur la base de l'authentification exécutée par un serveur d'autorisation, ainsi que d'obtenir des informations de base sur le profil de l'utilisateur final de manière interopérable et à la façon de services Internet.	*OpenID Foundation*	

technologie biométrique dans les projets d'administration électronique. Ce document, intitulé *Security Guidelines for Use of Biometric Technology in e-Governance Projects*, s'appuie sur les orientations énoncées dans les normes ISO 24745, ISO19792, ISO 24714 et ISO 24760.

Les normes encadrant la qualité des échantillons biométriques sont importantes pour s'assurer que les systèmes de reconnaissance automatique sont capables de lire les données biométriques recueillies. Une mauvaise qualité de l'échantillon risque en effet d'empêcher l'inscription et/ou de dégrader la performance globale de mise en correspondance des données biométriques. Sont concernées les normes internationales ISO/IEC 29794-4:2017 (données d'image de l'empreinte digitale), ISO/IEC TR 29794-5:2010 (données d'image du visage) et ISO/IEC 29794-6:2015 (données d'image de l'iris). L'Institut national des normes et de la technologie (NIST) des États-Unis a également publié des rapports sur la qualité d'image de l'empreinte digitale (NFIQ) et des SDK correspondants, utilisés partout dans le monde.

5.4 Cadres

La norme ISO/IEC 29115 et le règlement eIDAS définissent un cadre de niveaux de garantie pour les systèmes d'identification. Dans l'idéal, le système d'identification national devrait se conformer au niveau le plus élevé. Un débat plus approfondi sur ce thème faciliterait la préparation de lignes directrices sur les options pour la mise en œuvre de systèmes d'identification offrant les niveaux de garantie les plus élevés. Par ailleurs, des lignes directrices sur

N°	Domaine	Numéro de la norme	Description de la norme
1	Biométrie	Série ISO/IEC 29794	Qualité d'échantillon biométrique – Performance de comparaison et correspondance
2	Biométrie	Série ISO/IEC 29109	Méthodologie d'essai de conformité pour les formats d'interéchange de données biométriques
3	Biométrie	ISO/IEC 24745	Techniques de sécurité – Protection des informations biométriques
4	Biométrie	ISO/IEC 24761	Contexte d'authentification biométrique
5	Biométrie	NIST MINEX	Le *Minutiae Interoperability Exchange Test* (MINEX) est un programme du NIST pour l'exécution d'essais d'interopérabilité de générateurs et extracteurs de points caractéristiques de référence, pour le programme de vérification de l'identité des personnes (Personal Identity Verification – PIV) du gouvernement des États-Unis.
6	Biométrie	ISO/IEC 19784-1:2018	Spécification BioAPI
7	Biométrie	ISO/IEC 24709-1:2017	Test de conformité pour l'interface de programmation d'applications biométriques (BioAPI – ISO 19784)
8	Biométrie	ISO/IEC TR 29194:2015	Guide pour la mise au point de systèmes biométriques accessibles et inclusifs
9	Biométrie	ISO/IEC TR 29196:2015	Directives pour l'inscription biométrique
10	Biométrie	ISO/IEC TR 30125:2016	Biométrie utilisée avec des appareils mobiles
11	Biométrie	ISO 19792:2015	Techniques de sécurité – Évaluation de sécurité de la biométrie
12	Biométrie	ISO 24714:2015	Biométrie – Considérations juridictionnelles et sociétales pour applications commerciales – Partie 1 : orientations générales
13	Confidentialité	ISO/IEC 29100	Cadre du domaine privé
14	Confidentialité	ISO/IEC 27018	Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII
15	Confidentialité	ISO/IEC 29190	Modèle d'évaluation de l'aptitude à la confidentialité
16	Confidentialité	ISO/ IEC 29184	Lignes directrices concernant les déclarations de confidentialité en ligne et les consentements
17	Gestion	Série ISO/IEC 24760	Cadre pour la gestion de l'identité

les différentes options, indiquant leurs points forts et leurs points faibles et proposant plusieurs cas de figure en guise d'exemple, faciliteraient le choix du système d'identification approprié et des normes techniques applicables.

5.4.1 Niveaux de garantie

Lorsqu'une personne s'identifie ou s'authentifie au moyen d'un ou plusieurs attributs d'identité, le degré de certitude qu'elle est qui elle prétend être dépend du niveau de fiabilité et de sécurité fourni et du contexte dans lequel les informations sont capturées. C'est ce que l'on appelle le

Nom de la norme	Description de la norme	Organisme de normalisation	Observations
ISO/IEC 29115	Cadre d'assurance de l'authentification d'entité	ISO et IEC	Fixe quatre niveaux de garantie pour la gestion modulable de l´identité et les services d'authentification
FIDO UAF	Cadre d'authentification universel	Alliance FIDO	Authentification sans mot de passe
eIDAS	Identification électronique et services de confiance	Règlement européen	Règlement de l'Union européenne concernant l'identification et les services de confiance – Cadre d'interopérabilité des systèmes d'identification de l'UE

niveau de garantie. Les niveaux de garantie dépendent de la fiabilité des processus d'identification et d'authentification, et sont essentiels pour contrôler l'accès, assurer l'intégrité des données et limiter les risques de vols d'identité. Plus le niveau de garantie est élevé, plus faible est le risque que des prestataires de services se fondent sur un justificatif compromis lors d'une transaction. Pour établir l'identité, le niveau de garantie dépend de la méthode d'identification employée, notamment le périmètre des informations personnelles et des attributs recueillis à propos d'une personne lors de son inscription, et du degré de certitude avec lequel ces attributs sont vérifiés (autrement dit, validés). Par exemple, des données à caractère personnel recueillies lors de l'inscription mais non dédupliquées, ou dont la véracité n'est pas vérifiée par comparaison avec les bases de données existantes, donneront lieu à un niveau de garantie faible, en raison de l'absence de validation des informations d'identification.

La norme ISO/IEC 29115 définit un cadre d'assurance de l'authentification d'entité. Dans cette recommandation / norme internationale, l'assurance renvoie à la confiance placée dans l'ensemble des processus, activités de gestion et technologies employés pour établir et gérer l'identité d'une entité, pour les besoins des opérations d'authentification. Ce cadre recense en outre trois phases, alignées sur les trois grandes activités énumérées dans le cycle de vie de l'identification : l'inscription, l'accréditation et l'authentification. Il énumère également les activités organisationnelles et de gestion qui correspondent à la phase de gestion de l'identité, et considère les exigences en matière de fédération et le rôle du cadre d'assurance dans la même phase sans en faire un processus séparé.

La norme ISO 29115 fixe quatre niveaux de garantie, pour la gestion modulable de l´identité et les services d'authentification. Ces quatre niveaux sont présentés à la figure 5, avec les définitions correspondantes du cadre eIDAS de l'Union européenne, et vont des protocoles d'authentification faibles présentant des niveaux de risque de sécurité élevés aux protocoles d'authentification forts présentant des niveaux de risque minimaux. Le niveau de risque ne repose pas seulement sur les justificatifs et les processus utilisés pour l'authentification, mais également sur le degré de fiabilité avec lequel l'identité a été vérifiée lors de la phase d'enregistrement. Selon le type d'applications, les pays peuvent mettre en œuvre une diversité de protocoles d'authentification pour répondre aux normes nécessaires au cas d'espèce.

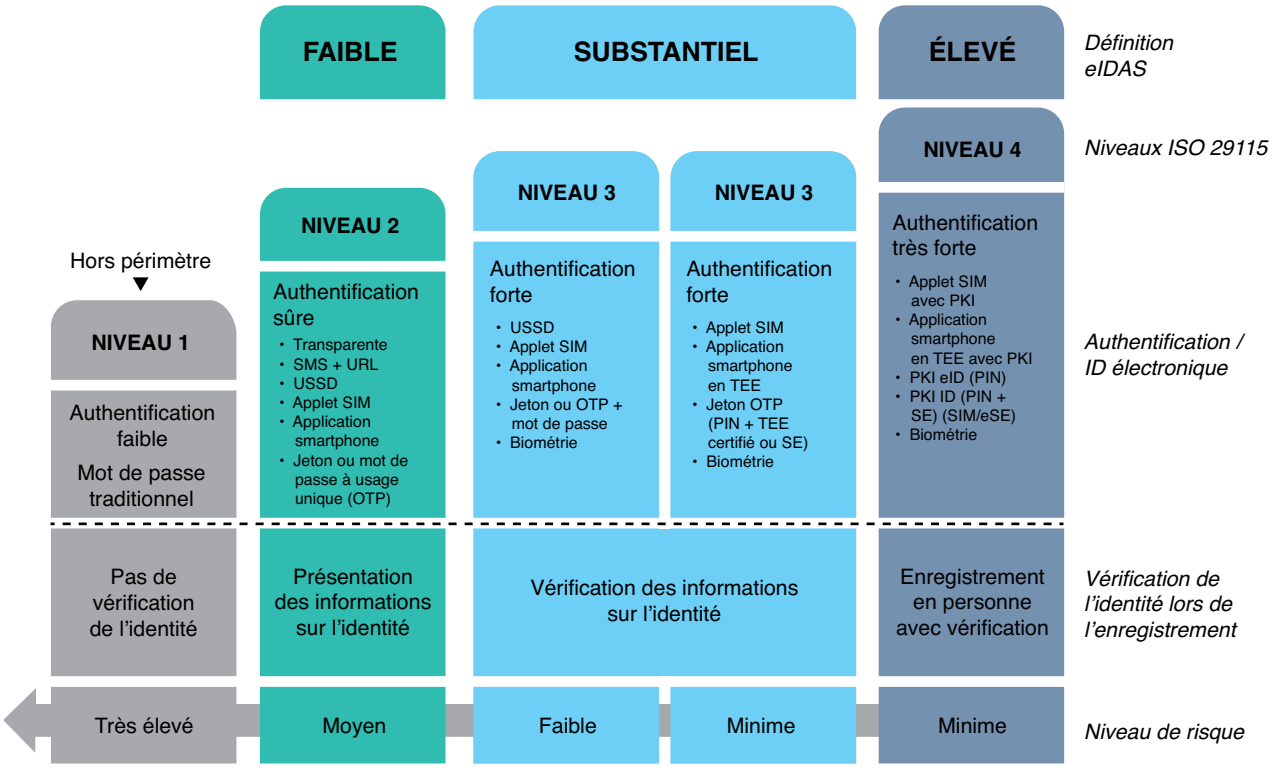
Les lignes directrices *Digital Identity Guidelines* 800-63-3 du NIST abrogent à partir de 2017 le concept de niveau de garantie comme échelle ordinale unique sur laquelle fonder les exigences propres à la mise en œuvre. Elles proposent trois catégories de garantie de l'identité distinctes, IAL, AAL et FAL, dans lesquelles les agences devront

sélectionner les niveaux de garantie voulus en conjuguant une gestion appropriée du risque opérationnel et de confidentialité et la prise en compte des besoins de la mission :

- IAL : processus de vérification de l'identité.
- AAL : processus d'authentification.
- FAL : fiabilité d'une affirmation dans un environnement fédéré, servant à communiquer des informations sur l'authentification et les attributs (s'il y a lieu) à une partie utilisatrice.

Certes, dans de nombreux systèmes, la valeur numérique sera la même dans les trois catégories. Il ne s'agit pour autant pas d'un impératif, et les agences ne doivent pas présupposer que ce sera le cas dans tout système donné. Cette distinction en trois catégories offre aux agences une certaine souplesse pour choisir leurs solutions d'identification. De plus, quel que soit le niveau de garantie, elle leur permet de mieux intégrer divers outils de renforcement de la protection de la vie privée en en faisant des éléments fondamentaux des systèmes d'identification. Ces lignes directrices, par exemple, proposent des scénarios qui permettront la réalisation de transactions sous pseudonyme, même en cas d'utilisation d'authentifiants forts et multi-facteurs. Elles visent en outre à limiter la diffusion des informations d'identification, en imposant aux fournisseurs d'identité fédérée d'accepter un éventail d'options pour l'interrogation des données. Il pourra s'agir d'une simple vérification de la conformité d´un attribut avec une règle fixée plutôt que de la transmission du détail des informations liées à l´attribut vérifié. Par exemple, le système confirmerait que l´individu a plus de 18 ans, sans transmettre la date de naissance au système. Certes, pour les agences, de nombreux scénarios d'utilisation exigeront l'identification complète des individus. Pour autant, ces lignes directrices encouragent l'accès sous pseudonyme aux services publics numériques chaque fois que possible, et, même si une identification complète est nécessaire, la limitation de la quantité d'informations à caractère personnel recueillies.

FIGURE 5 Niveaux d'authentification ISO et eIDAS



Source : Banque mondiale, 2016.

6. CAS D'UTILISATION PAYS

Selon l'environnement propre au pays, quelles sont les normes qu'il convient d'adopter et quelles sont celles qu'il est préférable d'ignorer ? La réponse dépend des objectifs, du champ d'application et de l'utilisation envisagée du système d'identification. Les exemples de l'Estonie, de l'Inde, du Malawi, du Pakistan et du Pérou présentés ci-dessous illustrent les normes applicables que les États concernés peuvent décider d'adopter pour répondre à leurs besoins. En élaborant un système d'identification, cependant, l'une des priorités est toujours de s'assurer que le choix des technologies et des normes connexes s'inscrit dans le cadre réglementaire en vigueur dans un pays.

Exemple 1: L'ID-Kaart en Estonie – Carte intelligente et carte d'identité sur mobile

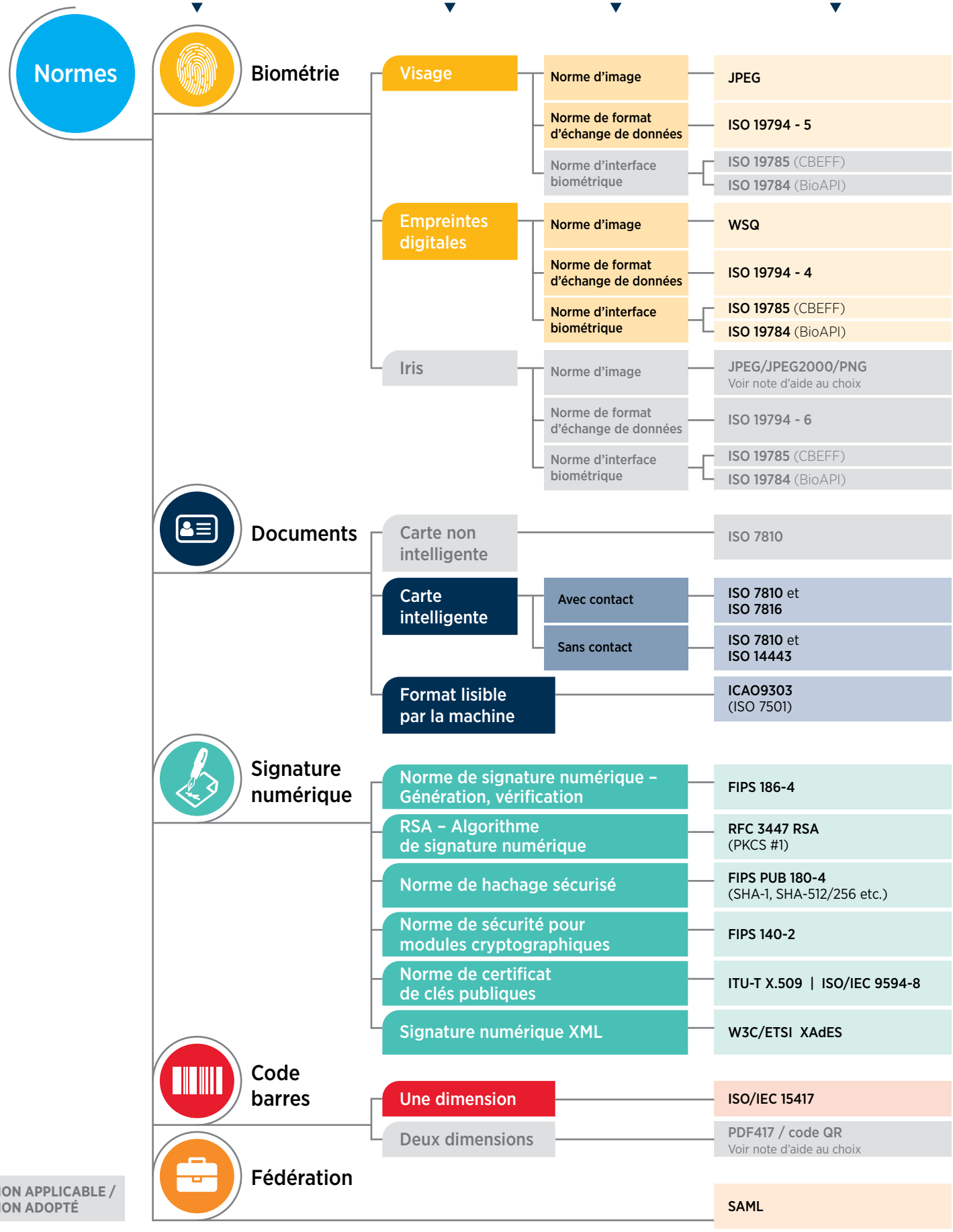
L'Estonie possède le système de carte d'identité nationale le plus développé du monde (Williams-Grut 2016). Le pays a délivré 1,3 million de ses ID-Kaarts intelligentes, chacune associée à un identifiant unique qui permet à son titulaire d'accéder à plus de 1 000 services publics, comme les services de santé, le dépôt des déclarations fiscales en ligne et le vote en ligne. À la pointe de la révolution numérique pour ce qui est des services publics, l'Estonie aspire à devenir un « pays en tant que service », dans lequel l'identité numérique sécurisée joue un rôle central. La puce intégrée dans la carte contient les principales données d'identification, comme le nom, la date de naissance, un numéro d'identification unique et des certificats numériques, pour authentification et signature numérique des documents. L'accès à chacune des clés de ces certificats numériques est protégé par un code PIN secret, que l'utilisateur est seul à connaître.

L'ID-Kaart possède des fonctions électroniques avancées qui facilitent l'authentification sécurisée et la création de signatures numériques juridiquement contraignantes utilisables pour accéder aux services en ligne dans tout le pays. L'infrastructure e-ID est modulable, souple, interopérable et fondée sur des normes. Tous les certificats délivrés en association avec le système de carte d'identité sont des certificats qualifiés, conformes à la directive européenne 1999/93/CE relative à l'utilisation des signatures électroniques dans les contrats électroniques au sein de l'Union européenne. La carte est conforme à la norme OACI 9303 relative aux documents de voyage. Le numéro d'identité personnel et le numéro d'identification du document sont encodés sous la forme de deux codes barres à une dimension, basés sur la norme ISO 15417. L'Estonie n´a pas recours à la déduplication biométrique pour délivrer une identité unique, mais prend les empreintes digitales au moment de la délivrance de la carte d'identité.

L'ID-Kaart est un justificatif sécurisé qui permet d'accéder aux services publics. Pour signer numériquement un document, le système a recours à un modèle de communication qui emploie des phases de travail normalisées sous la forme d'un format de document commun (DigiDoc). DigiDoc repose sur le format *Advanced Electronic Signatures Standard* (XAdES), ensemble d'extensions à la norme XML. XAdES définit un format qui permet le stockage structurel des données, signatures et attributs de sécurité associés aux signatures numériques, et favorise dès lors la compréhension commune et l'interopérabilité.

Source : e-Estonia.com et document intitulé *« The Estonian ID Card and Digital Signature Concept »* (version 20030307).

ESTONIE



NON APPLICABLE / NON ADOPTÉ

Exemple 2: Le système indien d'identification biométrique Aadhaar

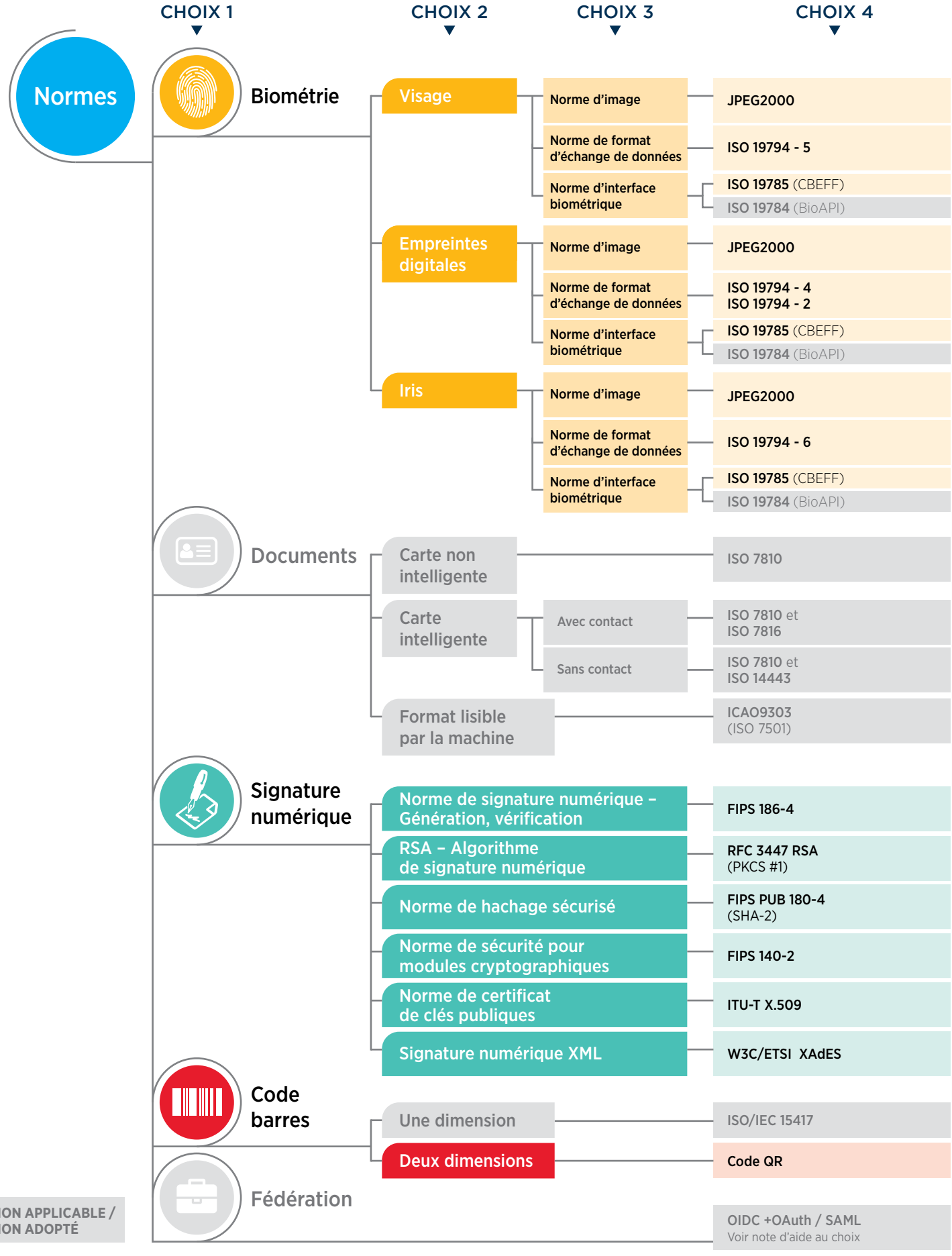
L'Autorité indienne de l'identification unique (UIDAI) a délivré un numéro d'identification unique, l'Aadhaar, à plus d'un milliard de résidents. La photographie, les empreintes digitales et l'iris de chaque résident sont captés avant la délivrance d'un Aadhaar. Il s'agit de la plus importante base de données biométriques multimodale du monde. En résultat de la mise en œuvre de ce système, près de la totalité de la population possède aujourd'hui une identité numérique. En 2009, l'UIDAI a mis en place un Comité de normalisation biométrique chargé de fixer le cap en matière de normes biométriques, proposer des bonnes pratiques et recommander des procédures biométriques pour le système. Le comité a recommandé la série ISO/IEC 19794 (parties 1, 2, 4, 5 et 6) et la norme ISO/IEC 19785 pour encadrer les formats d'échange de données biométriques et instaurer un cadre d'échange biométrique commun permettant de garantir l'interopérabilité. Le comité a retenu la norme ISO/IEC 15444 (toutes les parties) pour le système d'encodage (image JPEG 2000) de l'image du visage, des empreintes digitales et de l'iris.

En parallèle, l'UIDAI a pour principe de recourir à des logiciels libres, également utilisés avec succès aux États-Unis et en Europe. L´UIDAI a préparé le document en anglais *Security Guidelines for Use of Biometric Technology in e-Governance Projects (Lignes directrices pour l´utilisation de technologie biométriques dans les projets de gouvernement en ligne)* en s'appuyant sur les orientations énoncées dans les normes ISO 24745, ISO19792, ISO 24714 et ISO 24760. L'UIDAI a également proposé des normes (comité des normes démographiques) concernant les attributs saisis lors de l'enregistrement et ensuite utilisés pour l'authentification démographique. En outre, le système Aadhaar recourt largement aux solutions PKI/HSM pour le chiffrement des données pendant la transmission et le stockage et pour protéger l'accès à l'API.

Le système Aadhaar ne délivre pas de carte d'identité physique pour l'authentification. Une application mobile, mAadhaar, permet le stockage électronique des données démographiques (attributs relatifs à l´identité, tels que le nom, la date de naissance, etc.), du numéro Aadhaar et de la photographie sous la forme d'un code QR. Les résidents reçoivent également un document plastifié sur lequel figurent les données démographiques, la photo et le code QR (qui contient des données chiffrées et signées électroniquement). Le code QR figurant sur ce document papier ou dans l'application mAadhaar sert également dans certains cas à s'authentifier hors ligne, au moyen d'une application spécifique. L'authentification au moyen du numéro Aadhaar peut intervenir dans l'un ou plusieurs des modes ci-dessous, avec des réponses oui/non :

- Authentification démographique.
- Authentification biométrique.
- Authentification ponctuelle sur mobile avec PIN.
- L'authentification multifacteurs est une combinaison de deux ou trois des facteurs ci-dessus.

Source : site Internet de l'UIDAI et recommandations du Comité de normalisation biométrique 2009.

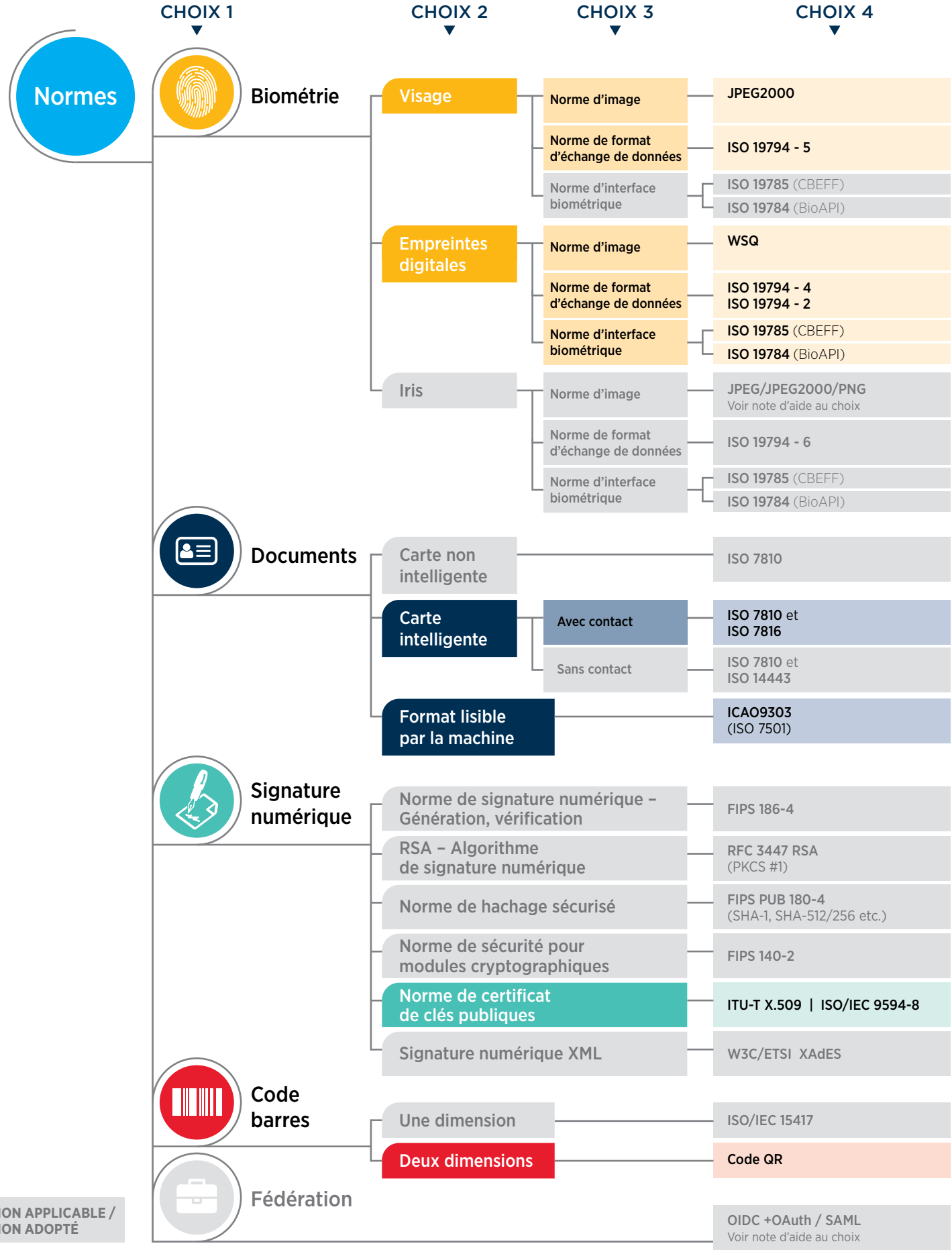

CHOIX 1
CHOIX 2
CHOIX 3
CHOIX 4
Normes
Biométrie
Visage
Norme d'image
JPEG2000
Norme de format d'échange de données
ISO 19794 - 5
Norme d'interface biométrique
ISO 19785 (CBEFF)
ISO 19784 (BioAPI)
Empreintes digitales
Norme d'image
JPEG2000
Norme de format d'échange de données
ISO 19794 - 4
ISO 19794 - 2
Norme d'interface biométrique
ISO 19785 (CBEFF)
ISO 19784 (BioAPI)
Iris
Norme d'image
JPEG2000
Norme de format d'échange de données
ISO 19794 - 6
Norme d'interface biométrique
ISO 19785 (CBEFF)
ISO 19784 (BioAPI)
Documents
Carte non intelligente
ISO 7810
Carte intelligente
Avec contact
ISO 7810 et ISO 7816
Sans contact
ISO 7810 et ISO 14443
Format lisible par la machine
ICAO9303 (ISO 7501)
Signature numérique
Norme de signature numérique – Génération, vérification
FIPS 186-4
RSA – Algorithme de signature numérique
RFC 3447 RSA (PKCS #1)
Norme de hachage sécurisé
FIPS PUB 180-4 (SHA-2)
Norme de sécurité pour modules cryptographiques
FIPS 140-2
Norme de certificat de clés publiques
ITU-T X.509
Signature numérique XML
W3C/ETSI XAdES
Code barres
Une dimension
ISO/IEC 15417
Deux dimensions
Code QR
Fédération
OIDC +OAuth / SAML
Voir note d'aide au choix
NON APPLICABLE / NON ADOPTÉ

Exemple 3: Malawi – Biométrie et carte intelligente

Le Malawi a récemment mis en place la couverture universelle de sa population adulte, en délivrant une carte d'identité nationale biométrique à 9 millions de personnes. L'opération s'est déroulée sous la supervision du Bureau national de l'enregistrement (NRB), relevant du ministère des Affaires intérieures et de la Sécurité nationale. Seuls les Malawiens de 16 ans ou plus reçoivent une carte d'identité nationale. Ceux de moins de 16 ans ont droit à un certificat de naissance national. La carte d'identité elle-même est particulièrement avancée. Le processus d'enregistrement permet la saisie de dix empreintes digitales, d'une photographie numérique et d'une signature électronique. La délivrance d'une carte d'identité intelligente unique intervient à la suite d'un exercice de déduplication biométrique. La carte d'identité est conforme aux normes OACI 9303 et ISO 7816, et intègre sept éléments de sécurité pour empêcher la falsification. Elle contient également un code QR.

L'applet Identity de l'OACI permettra aux titulaires de cette carte de s'en servir pour emprunter tous les vols intérieurs. Dans les aéroports, des lecteurs de cartes permettront d'accéder aux données et de vérifier l'identité du titulaire. La carte possède également un certificat numérique, délivré par le Bureau national de l'enregistrement. De la même manière, l'applet e-Health lui permettra de faire office de carte d'assurance maladie virtuelle (conforme à la norme européenne CWA15974), de sorte que les bureaux de santé pourront l'utiliser pour vérifier l'identité du titulaire et lui rendre les services auxquels il a droit. Cependant, si la carte d'identité nationale possède la capacité de faire office de carte d'assurance maladie, le ministère de la Santé n'a pas encore pris la décision qui lui permettra d'être utilisée à cet effet. Le cas échéant, les Malawiens ne seraient plus obligés de détenir une carte d'assurance maladie séparée, la carte d'identité nationale incorporant les principaux éléments de ce type de carte, en conformité avec les normes internationales observées par les pays européens, la Nouvelle-Zélande et l'Australie. L'applet KPI (infrastructure à clés publiques) donne aux pouvoirs publics les moyens de faire de cette carte le socle sur lequel déployer, par exemple, un programme d'inclusion financière ou de protection sociale et de vérifier l'identité des bénéficiaires. Pour terminer, l'applet e-Driver's License est capable de vérifier si le titulaire possède le permis de conduire.

Source : Tariq Malik, *Malawi's Journey Towards Transformation: Lessons from its National ID Project*, Center for Global Development (2018).

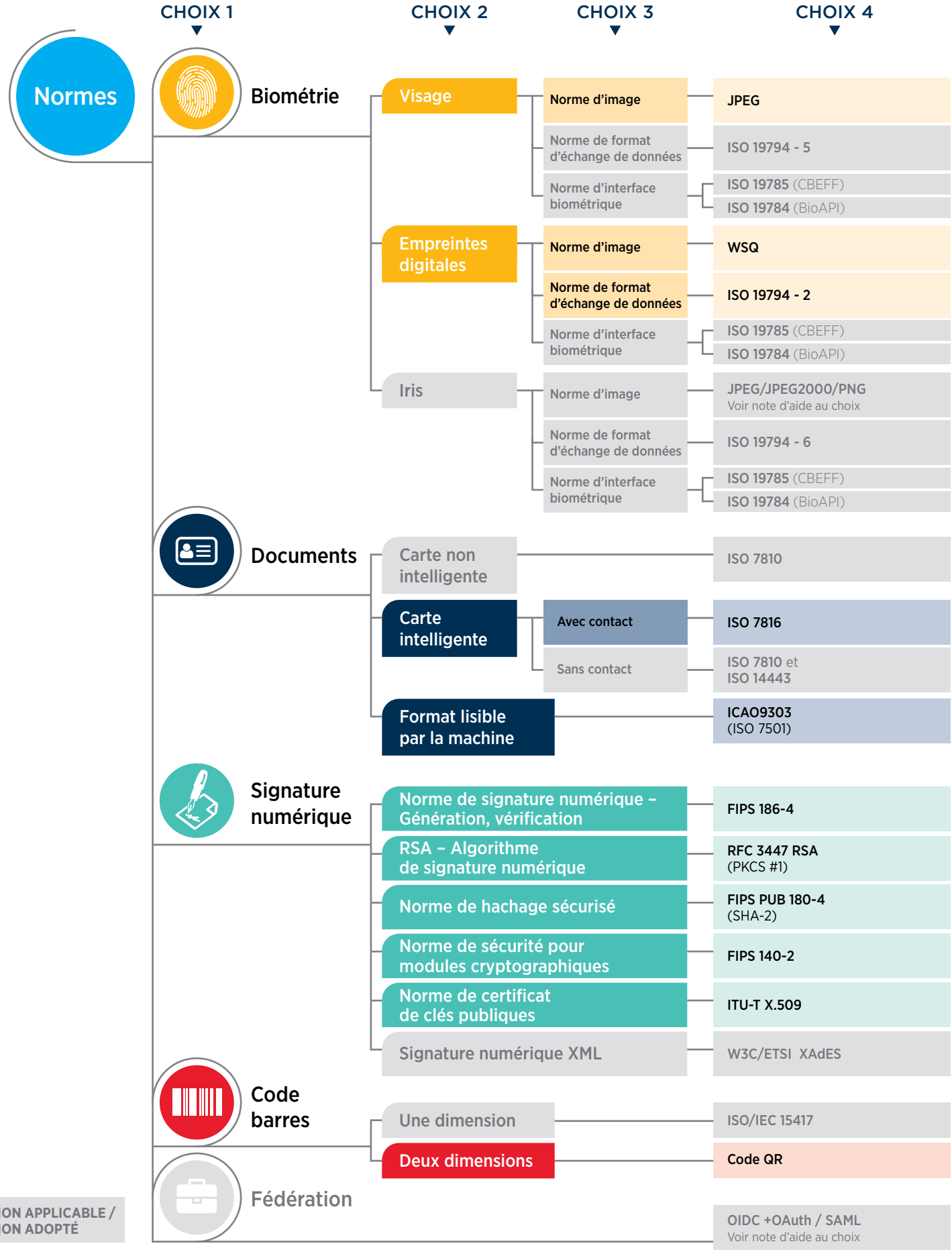

CHOIX 1
CHOIX 2
CHOIX 3
CHOIX 4
Normes
Biométrie
Visage
Norme d'image
JPEG2000
Norme de format d'échange de données
ISO 19794 - 5
Norme d'interface biométrique
ISO 19785 (CBEFF)
ISO 19784 (BioAPI)
Empreintes digitales
Norme d'image
WSQ
Norme de format d'échange de données
ISO 19794 - 4
ISO 19794 - 2
Norme d'interface biométrique
ISO 19785 (CBEFF)
ISO 19784 (BioAPI)
Iris
Norme d'image
JPEG/JPEG2000/PNG
Voir note d'aide au choix
Norme de format d'échange de données
ISO 19794 - 6
Norme d'interface biométrique
ISO 19785 (CBEFF)
ISO 19784 (BioAPI)
Documents
Carte non intelligente
ISO 7810
Carte intelligente
Avec contact
ISO 7810 et
ISO 7816
Sans contact
ISO 7810 et
ISO 14443
Format lisible par la machine
ICAO9303
(ISO 7501)
Signature numérique
Norme de signature numérique – Génération, vérification
FIPS 186-4
RSA – Algorithme de signature numérique
RFC 3447 RSA
(PKCS #1)
Norme de hachage sécurisé
FIPS PUB 180-4
(SHA-1, SHA-512/256 etc.)
Norme de sécurité pour modules cryptographiques
FIPS 140-2
Norme de certificat de clés publiques
ITU-T X.509 | ISO/IEC 9594-8
Signature numérique XML
W3C/ETSI XAdES
Code barres
Une dimension
ISO/IEC 15417
Deux dimensions
Code QR
Fédération
OIDC +OAuth / SAML
Voir note d'aide au choix
NON APPLICABLE / NON ADOPTÉ

Exemple 4: eID intelligente au Pakistan – Biométrie et carte intelligente

Avec plus de 121 millions de cartes d'identité délivrées, le NADRA, le service pakistanais en charge de la base de données nationale et de l'enregistrement, a enregistré 98 % de la population adulte de plus de 18 ans du pays. La carte d'identité pakistanaise a progressivement évolué au fil des années. C'est aujourd'hui une carte d'identité électronique intelligente, qui contient plusieurs attributs permettant de répondre aux enjeux d'un monde numérique et connecté. Le NADRA a conçu sa carte pour répondre également aux besoins des Pakistanais expatriés. En résultat, sa carte d'identité électronique intelligente destinée aux Pakistanais de l'étranger, la NICOP, est conforme à la norme OACI 9303, partie 3, volume 1, ainsi qu'à la norme ISO 7816-4. Une carte NICOP conforme aux normes de l'OACI est acceptée comme carte d'identité numérique dans tous les aéroports internationaux et aux points d'entrée et de sortie du territoire.

Le NADRA a également pour ligne directrice ou pour principe de recourir à des logiciels libres pour le développement des applications. Les données démographiques et les données biométriques sont utilisées en parallèle pour améliorer le processus de déduplication. Les services du NADRA en charge de la gestion de la qualité et de la production des cartes d'identité sont également certifiés ISO 9001:2000. La carte d'identité électronique intelligente intègre 20 éléments de sécurité apparents ou dissimulés pour éviter la falsification. Le verso comporte également un code QR et une zone à lecture automatique.

Source : analyse de l'auteur.

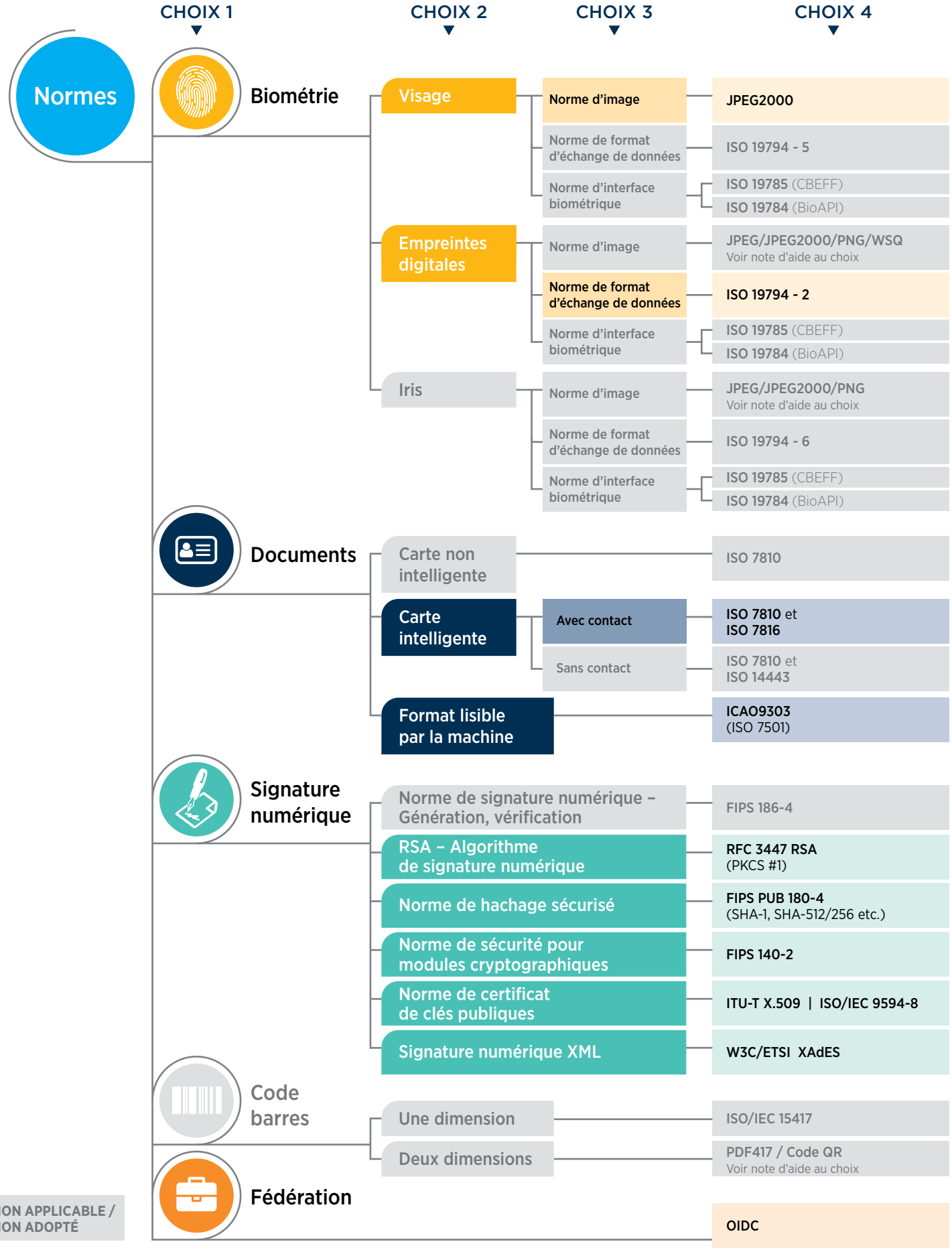

CHOIX 1
CHOIX 2
CHOIX 3
CHOIX 4
Normes
Biométrie
Visage
Norme d'image
JPEG
Norme de format d'échange de données
ISO 19794 - 5
Norme d'interface biométrique
ISO 19785 (CBEFF)
ISO 19784 (BioAPI)
Empreintes digitales
Norme d'image
WSQ
Norme de format d'échange de données
ISO 19794 - 2
Norme d'interface biométrique
ISO 19785 (CBEFF)
ISO 19784 (BioAPI)
Iris
Norme d'image
JPEG/JPEG2000/PNG
Voir note d'aide au choix
Norme de format d'échange de données
ISO 19794 - 6
Norme d'interface biométrique
ISO 19785 (CBEFF)
ISO 19784 (BioAPI)
Documents
Carte non intelligente
ISO 7810
Carte intelligente
Avec contact
ISO 7816
Sans contact
ISO 7810 et ISO 14443
Format lisible par la machine
ICAO9303 (ISO 7501)
Signature numérique
Norme de signature numérique – Génération, vérification
FIPS 186-4
RSA – Algorithme de signature numérique
RFC 3447 RSA (PKCS #1)
Norme de hachage sécurisé
FIPS PUB 180-4 (SHA-2)
Norme de sécurité pour modules cryptographiques
FIPS 140-2
Norme de certificat de clés publiques
ITU-T X.509
Signature numérique XML
W3C/ETSI XAdES
Code barres
Une dimension
ISO/IEC 15417
Deux dimensions
Code QR
Fédération
OIDC +OAuth / SAML
Voir note d'aide au choix
NON APPLICABLE / NON ADOPTÉ

Exemple 5: Carte d'identité électronique avec certificat numérique au Pérou

La carte d'identité nationale électronique péruvienne (DNIe) est délivrée par le Registre national de l'identification et de l'état civil (RENIEC). Le RENIEC, entité autonome dont les fonctions concernent l'état civil, l'identification et les signatures numériques, a délivré 30 millions de cartes d'identité électroniques à la quasi-totalité de la population du pays.

La carte d'identité électronique donne aux Péruviens une identité numérique qui peut être authentifiée de façon physique et virtuelle. Cette carte intègre deux certificats numériques qui permettent au titulaire de signer des documents électroniques avec la même valeur probante qu'une signature manuscrite. La carte d'identité électronique péruvienne est conforme à la norme ISO/IEC-7816, et son système biométrique à la norme ISO/IEC 19794. Également conforme à la norme OACI 9303, la carte sert aussi de document de voyage à lecture automatique (MRTD).

Source : entretien avec un représentant du RENIEC.


CHOIX 1
CHOIX 2
CHOIX 3
CHOIX 4
Normes
Biométrie
Visage
Norme d'image
JPEG2000
Norme de format d'échange de données
ISO 19794 - 5
Norme d'interface biométrique
ISO 19785 (CBEFF)
ISO 19784 (BioAPI)
Empreintes digitales
Norme d'image
JPEG/JPEG2000/PNG/WSQ
Voir note d'aide au choix
Norme de format d'échange de données
ISO 19794 - 2
Norme d'interface biométrique
ISO 19785 (CBEFF)
ISO 19784 (BioAPI)
Iris
Norme d'image
JPEG/JPEG2000/PNG
Voir note d'aide au choix
Norme de format d'échange de données
ISO 19794 - 6
Norme d'interface biométrique
ISO 19785 (CBEFF)
ISO 19784 (BioAPI)
Documents
Carte non intelligente
ISO 7810
Carte intelligente
Avec contact
ISO 7810 et ISO 7816
Sans contact
ISO 7810 et ISO 14443
Format lisible par la machine
ICAO9303 (ISO 7501)
Signature numérique
Norme de signature numérique – Génération, vérification
FIPS 186-4
RSA – Algorithme de signature numérique
RFC 3447 RSA (PKCS #1)
Norme de hachage sécurisé
FIPS PUB 180-4 (SHA-1, SHA-512/256 etc.)
Norme de sécurité pour modules cryptographiques
FIPS 140-2
Norme de certificat de clés publiques
ITU-T X.509 | ISO/IEC 9594-8
Signature numérique XML
W3C/ETSI XAdES
Code barres
Une dimension
ISO/IEC 15417
Deux dimensions
PDF417 / Code QR
Voir note d'aide au choix
Fédération
OIDC
NON APPLICABLE / NON ADOPTÉ

7. CONCLUSION

L'application de normes adéquates est déterminante pour exploiter tout le potentiel l'identité numérique et pour promouvoir la mise en œuvre d'une plateforme d'identité numérique qui soit interopérable, modulable, sûre et efficiente pour assurer la prestation des services. En l'absence de normes, il sera difficile de mettre en place des systèmes transversaux qui soient interopérables. Face au foisonnement des normes, il est primordial de savoir lesquelles adopter. La plupart des organismes normalisateurs chargés de mettre au point l'inscription biométrique, l'authentification, la délivrance et la gestion de l'identité participent aux comités techniques et aux groupes de travail de l'ISO, ce qui contribue grandement à l'acceptation des normes établies. Cependant, comme le montrent les exemples de pays présentés plus haut, le choix précis des normes applicables dépendra de la finalité, du champ d'application et de la fonction du système d'identification national, ainsi que du budget que les autorités sont disposées à consacrer à ces systèmes. Dans certains pays, la carte d'identité a des fonctions multiples, et peut servir notamment de permis de conduire, document de voyage et carte d'assurance maladie. Ce type de carte devra dès lors se conformer aux normes exigées par chaque fonction. Voir, par exemple, le cas du Malawi au chapitre 6.

Pour résumer, il est important de tenir compte de plusieurs considérations lors de la mise au point d'un système d'identification et de l'application de normes :

1. **Utiliser des normes ouvertes si possible.** Le recours à des normes ouvertes peut aider à garantir la fiabilité, l'interopérabilité et la neutralité technologique d'un système d'identification. Il importe cependant de se demander au préalable si la norme ouverte est largement utilisée sur le marché. La désaffection du marché pour certaines normes ouvertes peut traduire un problème de performance ou autre auquel il convient de réfléchir. Si une norme n'est pas largement utilisée, il pourra alors se révéler difficile d'assurer la mise en concurrence au moment de retenir un produit ou une solution potentiel. Une évaluation complète des besoins est indispensable avant de sélectionner les composantes de la solution. Lorsqu'une solution innovante est recherchée, le marché peut ne pas avoir adopté largement les normes applicables, si la solution est conçue pour répondre à des besoins ou à des enjeux particuliers notamment. De la même manière, dans les applications de niche, les forces du marché ne donneront qu'à une poignée de fournisseurs les moyens d'exister. Dans certaines situations, une solution fermée pourra également offrir de meilleurs résultats qu'une norme ouverte. Dans ce cas, la solution fermée pourra être la solution à privilégier. Il faudra alors s'assurer qu'elle ne débouche pas sur la dépendance à un seul fournisseur, en sélectionnant pour le système des composants qui prennent en charge des normes API ouvertes et permettent d'accéder aux données système dans des formats PDF ouverts (voir les normes sémantiques ci-dessous). Cette approche permettra également d'intégrer ou de supprimer des éléments du système à mesure que les fournisseurs changent ou que de nouvelles solutions plus efficientes se présentent. En outre, pour certaines fonctions d'un système d'identification autonomes et ne devant pas nécessairement être interopérables, comme la déduplication, on pourra privilégier le recours à une solution fermée, en supposant que la dépendance à un seul fournisseur ne pose pas de problème.
2. **Les normes techniques ne suffisent pas à elles seules.** Lors de la mise au point d'un système d'identification, outre l'application de normes techniques ouvertes, il importe également de tenir compte de normes sémantiques si l'on veut faciliter l'interopérabilité. Les normes sémantiques définissent les formats de données et les métadonnées pour les attributs d'identité comme le nom et la date de naissance (par exemple, le nombre de caractères autorisé pour un nom, l'ordre à respecter pour renseigner le prénom, le deuxième prénom et le nom ou le format de la date ou la date de naissance (mm/jj/aaaa ou jj/mm/aa). Leur but est de faciliter l'échange interopérable des données entre les systèmes. De plus, outre les normes techniques et sémantiques, de nombreux autres aspects sont à prendre en compte lors de la mise au point d'un système d'identification fiable, viable et inclusif. L'initiative ID4D a élaboré un éventail d'outils, dont un modèle permettant de chiffrer le coût d'un système d'identification notamment, capables d'aider à bien réfléchir à la conception d'un système. Un guide opérationnel prochainement publié sur le site de l'initiative ID4D (id4d.worldbank.org) présentera un résumé de ces outils.
3. **Se tourner vers l'avenir.** Les normes ne sont pas statiques. Elles évoluent dans le temps, à mesure que de nouvelles technologies émergent. Il est dès lors important de se tenir au courant des technologies émergentes et des nouvelles normes applicables aux systèmes d'identification. Il importe également d'en tenir compte en mettant au point un système d'identification, de manière à ne pas investir dans un système risquant de devenir rapidement obsolète ou de se révéler coûteux à optimiser au fur et à mesure de l'émergence de nouvelles technologies.

BIBLIOGRAPHIE

Ashiq, J. A. *The eIDAS Agenda: Innovation, Interoperability and Transparency.* Cryptomathic, consulté le 18 mars 2016.

Banque mondiale. *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation.* ID4D. 2016.

Banque mondiale. *Technology Landscape for Digital Identification.* ID4D. 2018).

ENISA. *Mobile ID Management.* European Network and Information Security Agency, consulté le 11 avril 2016.

Europa.eu. *Règlements, directives et autres actes législatifs.* Union européenne, consulté le 18 mars 2016.

Fumy, Walter, et Manfred Paeschke. *Handbook of eID Security: Concepts, Practical Experiences, Technologies.* John Wiley & Sons, 13 décembre 2010.

Gelb, Alan, et Julia Clark. *Identification for Development: The Biometrics Revolution.* Working Paper, Washington, DC: Center for Global Development, 2013.

Gomes de Andrade, Norberto Nuno, Shara Monteleone, et Aaron Martin. *Electronic Identity in Europe: Legal Challenges and Future Perspectives (eID 2020).* Centre commun de recherche, Commission européenne, 2013.

GSMA et SIA. *Mobile Identity—Unlocking the Potential of the Digital Economy.* Groupe Spécial Mobile Association (GSMA) et Secure Identity Alliance, octobre 2014.

IEEE. *What Are Standards? Why Are They Important?* IEEE, 2011. http://standardsinsight.com/ieee_company_detail/what-are-standards-why-are-they-important.

PIRA. *The Future of Personal ID to 2019.* Smithers PIRA International, 6 juin 2014.

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 au sein du marché intérieur et abrogeant la directive 1999/93/CE.

Turner, Dawn M. *eIDAS from Directive to Regulation—Legal Aspects.* Cryptomathic, consulté le 18 mars 2016.

Turner, Dawn M. *Understanding Major Terms Around Digital Signatures.* Cryptomathic, consulté le 18 mars 2016.

UIT. *Biometrics and Standards.* Secteur de la normalisation des télécommunications, Union internationale des télécommunications, consulté le 11 avril 2016.

UIT. *Biometric Standards: ITU-T Technology Watch Report.* Union internationale des télécommunications, décembre 2009.

van Zijp, Jacques. *Is the EU Ready for eIDAS?* Secure Identity Alliance, consulté le 18 march 2016.

Williams-Grut, Oscar. « Estonia wants to become a 'country as a service'. » *Business Insider*, 2016.

ANNEXE A
COMITÉS TECHNIQUES MIXTES, SOUS-COMITÉS ET GROUPES DE TRAVAIL DE L'ISO/IEC ET LEUR MANDAT

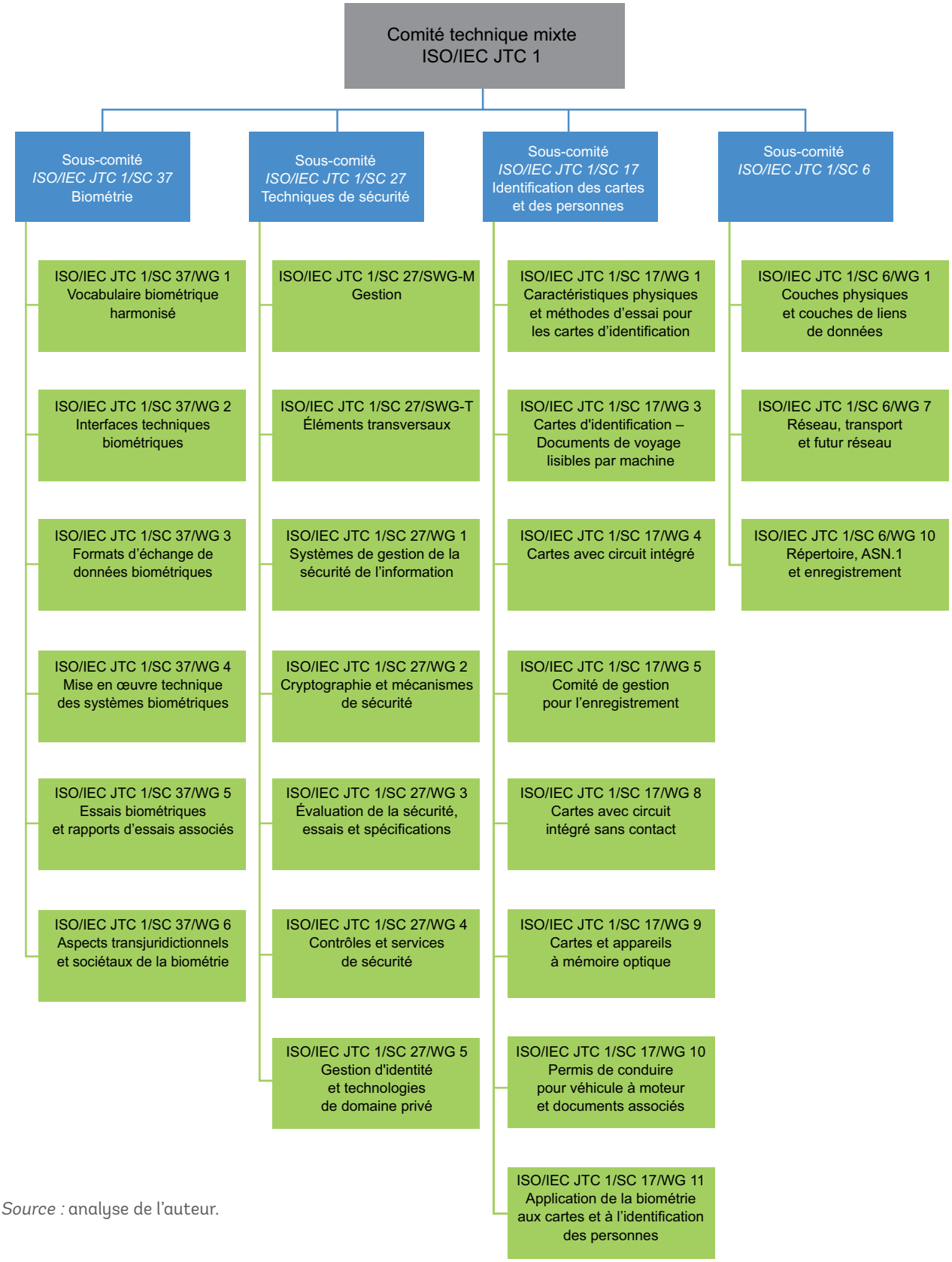
Comités techniques et groupes de travail de l'ISO

L'ISO a créé des comité techniques, sous-comités et groupes de travail en communication permanente avec d'autres organisations nationales et internationales, ainsi qu'avec les consortiums d'entreprises prenant part à l'examen ou à la définition des normes. L'ISO et la Commission électrotechnique internationale ont formé un comité technique mixte, dénommé ISO/IEC JTC 1, pour assurer partout dans le monde une approche globale de l'élaboration et de l'approbation de normes biométriques internationales. Au sein du JTC 1, les sous-comités 37, 27 et 17 concernent tous les pays qui prévoient d'instaurer un système d'identité numérique. Les sous-comités se répartissent en divers groupes de travail, chargés d'élaborer et d'actualiser les normes propres au cycle de vie de l'identité numérique :

1. ISO/IEC JTC 1/SC 37 : Biométrie
2. ISO/IEC JTC 1/SC 27 : Techniques de sécurité des technologies de l'information
3. ISO/IEC JTC 1/SC 17 : Identification des cartes et des personnes
4. ISO/IEC JTC 1/SC 6 : Télécommunications et échange d'informations entre les systèmes (normes sur la signature numérique / PKI)

Ces sous-comités travaillent avec d'autres sous-comités au sein de l'ISO (comités de liaison), ainsi qu'avec des organisations externes (organisations en liaison), dont certaines prennent part à l'élaboration de normes connexes. Le tableau ci-dessous indique le rôle, le champ d'action et le mandat des sous-comités techniques et de leurs groupes de travail.

FIGURE 6 ISO/IEC JTC 1 : Sous-comités et groupes de travail en charge de la gestion de l'identité



Source : analyse de l'auteur.

Sous-comités / Groupes de travail	Domaine de travail	Description
ISO/IEC JTC 1/SC 37 Biométrie	Normalisation des technologies biométriques génériques concernant les êtres humains pour faciliter l'interopérabilité et l'échange de données parmi les applications et les systèmes.	Cadres de fichiers communs, interfaces de programmation d'applications biométriques (BioAPI), formats d'échange de données biométriques, profils biométriques connexes, application de critères d'évaluation aux technologies biométriques, méthodologies concernant les essais de performance et les rapports d'essais associés et les aspects transjuridictionnels et sociétaux.
ISO/IEC JTC 1/SC 37/WG 1	Vocabulaire biométrique harmonisé	
ISO/IEC JTC 1/SC 37/WG 2	Interfaces techniques biométriques	
ISO/IEC JTC 1/SC 37/WG 3	Formats d'échange de données biométriques	
ISO/IEC JTC 1/SC 37/WG 4	Mise en œuvre technique des systèmes biométriques	
ISO/IEC JTC 1/SC 37/WG 5	Essais biométriques et rapports d'essais associés	
ISO/IEC JTC 1/SC 37/WG 6	Aspects transjuridictionnels et sociétaux de la biométrie	
ISO/IEC JTC 1/SC 27 IT Techniques de sécurité	Élaboration de normes pour la protection de l'information et des technologies de l'information et des communications (TIC). Le domaine de travail englobe les méthodes, techniques et lignes directrices de nature générale destinées à répondre aux aspects de sécurité et de protection de la vie privée. 1) Méthode pour cerner les impératifs de sécurité ; 2) Gestion de la sécurité de l'information et des TIC, et notamment les systèmes de gestion de la sécurité de l'information, du processus de sécurité, des contrôles et services de sécurité ; 3) Mécanismes de sécurité cryptographiques et autres, et notamment, sans pour autant s'y limiter, les mécanismes permettant d'assurer le contrôle, la disponibilité, l'intégrité et la confidentialité des informations ; 4) Documentation d'appui à la gestion de la sécurité, notamment la terminologie, les lignes directrices et les procédures d'enregistrement des éléments de sécurité ; 5) Aspects liés à la sécurité de la gestion de l'identité, de la biométrie et de la protection de la vie privée ; 6) Évaluation de la conformité, des impératifs d'accréditation et de contrôle dans le domaine des systèmes de gestion de la sécurité de l'information ; 7) Critères et méthodes pour l'évaluation de la sécurité.	Élaboration de normes internationales, rapports techniques et cahiers des charges techniques dans le domaine de la sécurité de l'information et des technologies de l'information. Les activités de normalisation de ce sous-comité comprennent les méthodes générales, les impératifs des systèmes de gestion, les techniques et les lignes directrices en vue d'assurer la sécurité et la confidentialité de l'information.
ISO/IEC JTC 1/SC 27/SWG-M	Gestion	
ISO/IEC JTC 1/SC 27/SWG-T	Éléments transversaux	
ISO/IEC JTC 1/SC 27/WG 1	Systèmes de gestion de la sécurité de l'information	
ISO/IEC JTC 1/SC 27/WG 2	Cryptographie et mécanismes de sécurité	
ISO/IEC JTC 1/SC 27/WG 3	Évaluation de la sécurité, essais et spécifications	
ISO/IEC JTC 1/SC 27/WG 4	Contrôles et services de sécurité	
ISO/IEC JTC 1/SC 27/WG 5	Gestion d'identité et technologies de domaine privé	
ISO/IEC JTC 1/SC 17 Identification des cartes et des personnes	Normalisation concernant les documents d'identification et documents associés, les cartes et les appareils associés à leur utilisation dans les applications intersectorielles et l'échange international	Élabore et facilite les normes dans le domaine des cartes d'identification et de l'identification des personnes

Sous-comités / Groupes de travail	Domaine de travail	Description
ISO/IEC JTC 1/SC 17/WG 1	Caractéristiques physiques et méthodes d'essais pour les cartes d'identification	
ISO/IEC JTC 1/SC 17/WG 3	Cartes d'identification - Documents de voyage lisibles par machine	
ISO/IEC JTC 1/SC 17/WG 4	Cartes avec circuit intégré avec contacts	
ISO/IEC JTC 1/SC 17/WG 5	Comité de gestion pour l'enregistrement (RMG)	
ISO/IEC JTC 1/SC 17/WG 8	Cartes avec circuit intégré sans contact	
ISO/IEC JTC 1/SC 17/WG 9	Cartes et appareils à mémoire optique	
ISO/IEC JTC 1/SC 17/WG 10	Permis de conduire pour véhicule à moteur et documents associés	
ISO/IEC JTC 1/SC 17/WG 11	Application de la biométrie aux cartes et à l'identification des personnes	

Source : ISO http://www.iso.org/iso/home.htm.