Union internationale des télécommunications

# UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

# X.1403

(09/2020)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Applications et services sécurisés (2) – Sécurité de la technologie des registres distribués

# Lignes directrices sur la sécurité relatives à l'utilisation de la technologie des registres distribués pour la gestion décentralisée des identités

Recommandation UIT-T X.1403

RECOMMANDATIONS UIT-T DE LA SÉRIE X

**RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ**

| | |
|---|---|
| RÉSEAUX PUBLICS DE DONNÉES | X.1–X.199 |
| INTERCONNEXION DES SYSTÈMES OUVERTS | X.200–X.299 |
| INTERFONCTIONNEMENT DES RÉSEAUX | X.300–X.399 |
| SYSTÈMES DE MESSAGERIE | X.400–X.499 |
| ANNUAIRE | X.500–X.599 |
| RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES | X.600–X.699 |
| GESTION OSI | X.700–X.799 |
| SÉCURITÉ | X.800–X.849 |
| APPLICATIONS OSI | X.850–X.899 |
| TRAITEMENT RÉPARTI OUVERT | X.900–X.999 |
| SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX | |
| Aspects généraux de la sécurité | X.1000–X.1029 |
| Sécurité des réseaux | X.1030–X.1049 |
| Gestion de la sécurité | X.1050–X.1069 |
| Télébiométrie | X.1080–X.1099 |
| APPLICATIONS ET SERVICES SÉCURISÉS (1) | |
| Sécurité en multidiffusion | X.1100–X.1109 |
| Sécurité des réseaux domestiques | X.1110–X.1119 |
| Sécurité des télécommunications mobiles | X.1120–X.1139 |
| Sécurité de la toile | X.1140–X.1149 |
| Protocoles de sécurité (1) | X.1150–X.1159 |
| Sécurité d'homologue à homologue | X.1160–X.1169 |
| Sécurité des identificateurs en réseau | X.1170–X.1179 |
| Sécurité de la télévision par réseau IP | X.1180–X.1199 |
| SÉCURITÉ DU CYBERESPACE | |
| Cybersécurité | X.1200–X.1229 |
| Lutte contre le spam | X.1230–X.1249 |
| Gestion des identités | X.1250–X.1279 |
| APPLICATIONS ET SERVICES SÉCURISÉS (2) | |
| Communications d'urgence | X.1300–X.1309 |
| Sécurité des réseaux de capteurs ubiquitaires | X.1310–X.1319 |
| Sécurité des réseaux électriques intelligents | X.1330–X.1339 |
| Courrier certifié | X.1340–X.1349 |
| Sécurité de l'Internet des objets (IoT) | X.1360–X.1369 |
| Sécurité des systèmes de transport intelligents | X.1370–X.1389 |
| **Sécurité de la technologie des registres distribués** | **X.1400–X.1429** |
| Sécurité de la technologie des registres distribués | X.1430–X.1449 |
| Protocoles de sécurité (2) | X.1450–X.1459 |
| ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ | |
| Aperçu général de la cybersécurité | X.1500–X.1519 |
| Échange concernant les vulnérabilités/les états | X.1520–X.1539 |
| Échange concernant les événements/les incidents/l'heuristique | X.1540–X.1549 |
| Échange de politiques | X.1550–X.1559 |
| Heuristique et demande d'informations | X.1560–X.1569 |
| Identification et découverte | X.1570–X.1579 |
| Échange garanti | X.1580–X.1589 |
| SÉCURITÉ DE L'INFORMATIQUE EN NUAGE | |
| Aperçu de la sécurité de l'informatique en nuage | X.1600–X.1601 |
| Conception de la sécurité de l'informatique en nuage | X.1602–X.1639 |
| Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage | X.1640–X.1659 |
| Mise en œuvre de la sécurité de l'informatique en nuage | X.1660–X.1679 |
| Sécurité de l'informatique en nuage (autres) | X.1680–X.1699 |
| COMMUNICATIONS QUANTIQUES | |
| Terminologie | X.1700–X.1701 |
| Générateur quantique de nombres aléatoires | X.1702–X.1709 |
| Cadre de sécurité pour les réseaux QKDN | X.1710–X.1711 |
| Conception de la sécurité pour les réseaux QKDN | X.1712–X.1719 |
| Techniques de sécurité pour les réseaux QKDN | X.1720–X.1729 |
| SÉCURITÉ DES DONNÉES | |
| Sécurité des mégadonnées | X.1750–X.1759 |
| SÉCURITÉ DE LA 5G | X.1800–X.1819 |

*Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.*

# Recommandation UIT-T X.1403

## Lignes directrices sur la sécurité relatives à l'utilisation de la technologie des registres distribués pour la gestion décentralisée des identités


**Résumé**

La technologie des registres distribués (DLT) et ses applications spécifiques telles que la blockchain offrent une opportunité unique d'utiliser une infrastructure de confiance et une plate-forme qui pourraient s'avérer utiles en permettant à une fédération de confiance d'échanger des attributs d'identité et des informations d'identité. La Recommandation UIT-T X.1403 définit les aspects de confidentialité et de sécurité propres aux télécommunications dans l'utilisation de données DLT pour la gestion des identités.



**Historique**

| Édition | Recommandation | Approbation | Commission d'études | Identifiant unique* |
|---|---|---|---|---|
| 1.0 | UIT-T X.1403 | 03-09-2020 | 17 | 11.1002/1000/14264 |

**Mots clés**

Technologie des registres distribués, gestion des identités


* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

## AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

## NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et on considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

## DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

## TABLE DES MATIÈRES

# Recommandation UIT-T X.1403

# Lignes directrices pour la sécurité relatives à l'utilisation de la technologie des registres distribués pour la gestion décentralisée des identités

## 1 Domaine d'application

La technologie des registres distribués (DLT) fournit une infrastructure de confiance qui permet à des systèmes de gestion décentralisée des identités d'échanger des attributs d'identité et des informations d'identité.

La présente Recommandation donne un aperçu de l'utilisation de la technologie DLT pour la gestion décentralisée des identités. Elle comprend notamment:

– un bref aperçu de l'utilisation des registres distribués pour la gestion des identités et des données d'identité;

– une analyse des avantages en termes de sécurité des identités décentralisées;

– des orientations concernant les contrôles nécessaires qui devraient être exécutés pour atténuer les menaces pesant sur les données d'identité.

## 2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T X.1252] Recommandation UIT-T X.1252 (2010), *Termes et définitions de base relatifs à la gestion d'identité.*

[UIT-T X.1254] Recommandation UIT-T X.1254 (2012), *Cadre de garantie d'authentification des entités.*

[UIT-T X.1277] Recommandation UIT-T X.1277 (2018), *Cadre d'authentification universelle.*

[UIT-T X.1278] Recommandation UIT-T X.1278 (2018), *Protocole client-authentificateur/Cadre applicable au double facteur universel.*

## 3 Définitions

### 3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

**3.1.1 déclaration** [UIT-T X.1252]: fait d'affirmer être le cas, sans pouvoir fournir de preuve.

**3.1.2 justificatifs** [UIT-T X.1252]: ensemble de données présentées comme preuve d'une identité et/ou d'une habilitation affirmées.

**3.1.3 document DID** [b-W3C-2]: ensemble de données décrivant le sujet du DID, y compris les mécanismes, tels que les clés publiques et le pseudonyme biométrique, que le sujet du DID peut utiliser pour s'authentifier et justifier qu'il y a correspondance avec le DID.

**3.1.4 entité** [UIT-T X.1252]: élément qui a une existence séparée et distincte et peut être identifié dans un contexte.

**3.1.5 fédération** [UIT-T X.1252]: association d'utilisateurs, de fournisseurs de service et de fournisseurs de service d'identité.

**3.1.6 fournisseur de service d'identité (IdSP)** [UIT-T X.1252]: entité qui vérifie, tient à jour, gère, peut créer et attribuer des informations d'identité concernant d'autres entités.

## 3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

**3.2.1 identificateur décentralisé (DID)**: identificateur unique à l'échelle mondiale ne nécessitant pas d'autorité centrale d'enregistrement étant donné qu'il est enregistré avec la technologie des registres distribués (DLT) ou une autre forme de système décentralisé.

NOTE – Définition établie à partir de celle figurant dans la norme [b-W3C-2].

**3.2.2 sujet du DID**: entité dont traite le document DID. C'est-à-dire l'entité identifiée par le DID et décrite par le document DID.

NOTE – Définition établie à partir de celle figurant dans la norme [b-W3C-2].

**3.2.3 porte-clés**: désigne la tâche de sécurisation du stockage de clés privées ou de données sur une unité matérielle de confiance dans un dispositif.

**3.2.4 point d'extrémité de service**: adresse de registre distribué à laquelle un service opère pour le compte d'un sujet du DID. Parmi les services spécifiques figurent les services de découverte, les réseaux sociaux, les services de stockage de fichiers et les services de dépôt de déclarations contrôlables. Les points d'extrémité de service peuvent également être fournis par un protocole d'échange de données généralisé, tel que l'échange de données extensible.

NOTE – Définition établie à partir de celle figurant dans la norme [b-W3C-2].

**3.2.5 cadre de confiance**: ensemble de spécifications, règles et accords ayant force exécutoire présidant à un système de gestion des identités.

**3.2.6 portefeuille (portefeuille d'identité)**: application permettant à l'utilisateur de détenir des identifiants et des justificatifs en stockant les clés privées correspondantes sur le dispositif de l'utilisateur.

**3.2.7 justificatif à apport nul de connaissance**: justificatif utilisant une cryptographie spéciale et un secret maître pour autoriser la divulgation sélective d'information dans un ensemble de déclarations. Un justificatif à apport nul de connaissance prouve qu'une partie ou la totalité des données d'un ensemble de déclarations est vraie sans révéler d'information additionnelle, y compris l'identité du démonstrateur.

# 4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

DDO document DID (*DID document*)

DID identificateur décentralisé *(decentralized identifier)*

DIdAm gestion d'identité et d'accès décentralisée *(decentralized identity and access management)*

DLT technologie des registres distribués *(distributed ledger technology)*

IdAM gestion d'identité et d'accès *(identity access and management)*

IdSP fournisseur de service d'identité *(identity service provider)*

IT technologies de l'information *(information technology)*

PKI infrastructure de clé publique *(public key infrastructure)*

PII informations d'identification personnelle *(personally identifiable information)*

RP partie utilisatrice *(relying party)*

SAML langage de balisage d'assertion de sécurité *(security assertion markup language)*

SP fournisseur de services (*service provider*)

SSI identité auto-souveraine *(self-sovereign identity)*

SSO authentification unique *(single sign-on)*

URL localisateur uniforme de ressource *(uniform resource locator)*

## 5 Conventions

La présente Recommandation emploie les formes des verbes ci-après lors de la formulation des dispositions:

a) "doit" désigne une obligation,

b) "devrait" désigne une recommandation,

c) "peut" désigne une autorisation,

d) "pourrait" désigne une possibilité ou une capacité.

## 6 Vers l'identité numérique décentralisée

La technologie des registres distribués joue un rôle essentiel dans la progression de l'évolution et de la maturité des systèmes d'identité décentralisés.

La multiplication des dispositifs mobiles et de l'Internet des objets accroît la pression sur les systèmes de gestion d'identité et d'accès classiques (IdAM) à évoluer vers des plates-formes agiles et intelligentes capables de prendre en charge des systèmes mobiles et informatiques dématérialisés (informatique en nuage).

Les systèmes de gestion d'identité et d'accès classiques sont mis en œuvre au-dessus d'autorités centralisées telles que les services d'annuaires d'entreprise, les autorités de certification ou les registres de noms de domaines. Chacune de ces autorités centralisées à l'échelle d'une organisation constitue son propre domaine de confiance. Au sein d'un système IdAM classique, l'autorité centralisée peut représenter un point de panne unique. La fédération des identités [UIT-T X.1252] est apparue comme une solution palliative qui permettait à des systèmes IdAM d'interagir, chacune des différentes organisations contrôlant ses propres domaines respectifs.

L'émergence de la technologie DLT offre l'opportunité de développer des solutions de gestion d'identité et d'accès décentralisée (DIdAm). La technologie DLT fournit un moyen de gérer la confiance sans autorité centralisée évitant ainsi tout point de panne isolé éventuel. En outre, la technologie DLT permet à chaque entité de créer et de gérer ses propres identificateurs sur n'importe quel nombre de registres distribués.

Les modèles d'identité numérique n'ont cessé d'évoluer pour s'adapter à l'évolution des besoins d'activité. Il existe trois modèles d'identité de base décrits au § 6.

### 6.1 Modèle d'identité centralisé

Il s'agit du modèle d'identité numérique le plus ancien et le plus utilisé actuellement [UIT-T X.1252]. Dans un modèle d'identité centralisé, les organisations font office de fournisseur de service d'identité (IdSP). Au sein de ce modèle, une organisation établit une relation de confiance point à point avec chacun de ses utilisateurs. Il s'agit d'un modèle classique cloisonné dans lequel une organisation émet un justificatif à un utilisateur qui autorise ce dernier à accéder aux services de l'organisation.

Dans ce modèle, chaque organisation fait office de fournisseur IdSP. L'organisation gère l'identité numérique de l'utilisateur et décide des relations de confiance acceptées. La confiance entre l'utilisateur et le fournisseur IdSP s'établit généralement par l'utilisation de secrets partagés tels que l'utilisation d'un nom d'utilisateur et d'un mot de passe. Dans certains cas, les secrets partagés sont complétés par des authentifications à plusieurs facteurs telles que des jetons, des données biométriques ou des solutions fondées sur le cadre d'authentification FIDO [UIT-T X.1277] et [UIT-T X.1278].

Dans un modèle centralisé, le fournisseur IdSP peut stocker et recueillir des données concernant les utilisateurs. Ces données peuvent être monétisées, partagées ou vendues à d'autres parties selon le modèle économique du fournisseur de service d'identité (IdSP). Les utilisateurs doivent se fier au fait que le fournisseur IdSP gèrera leurs données comme il se doit. Bien que les utilisateurs bénéficient des services de l'organisation, dans la plupart des cas, ils n'ont pas le contrôle sur la gestion de leurs propres identités, données personnelles et attributs d'identité. Dans ce modèle, le fournisseur IdSP est le propriétaire de l'identité de l'utilisateur. Les utilisateurs n'ont pas la capacité de transférer leurs données à d'autres fournisseurs.

Au sein d'un modèle d'identité centralisé, l'utilisateur est amené à créer et à gérer des justificatifs distincts pour chacune de ses relations commerciales avec chacun des fournisseurs IdSP. Une organisation exige la création de ces justificatifs avant d'autoriser un utilisateur à accéder à ses ressources. Ce modèle submerge l'utilisateur par une multitude d'identités en ligne. Le manque d'authentification mutuelle lors de l'identification rend ce modèle vulnérable aux attaques par hameçonnage et collecte de justificatifs. Ce modèle encourage l'utilisateur à réutiliser des mots de passe, ce qui augmente encore les risques de sécurité et les vulnérabilités.

Le modèle centralisé fait peser une lourde charge sur le fournisseur IdSP en matière de gestion du cycle de vie de l'identité. Ce modèle requiert notamment que chaque fournisseur IdSP procède à la vérification de l'identité [UIT-T X.1254] au cours de la phase d'inscription dans la gestion du cycle de vie de l'identité. La vérification d'identité est nécessaire afin d'établir un niveau de confiance dans l'identité déclarée. Ce processus peut se répéter tout au long du cycle de vie d'une identité donnée. Cette étape est problématique du point de vue de l'utilisateur, car le modèle centralisé requiert que l'utilisateur passe par l'étape de vérification de l'identité séparément pour chaque fournisseur d'identité. En outre, la menace de violation des données augmente les risques de piratage de comptes sachant que les organisations s'appuient sur des banques de données centralisées qui sont régulièrement prises pour cible par les pirates.

### 6.2 Modèle d'identité fédéré

Les organisations ont constaté les limites du modèle d'identité centralisé comme évoqué au § 6.1 et pris des mesures pour développer le modèle d'identité fédéré afin de répondre à ces problématiques. Le modèle d'identité fédéré vise à réduire la charge pesant sur les utilisateurs en permettant à ces derniers de transférer leur identité d'un domaine à un autre. Le langage de balisage d'assertion de sécurité (SAML) [UIT-T X.1242] présente une plus grande simplicité d'utilisation pour les personnes, grâce à une fonction d'authentification unique (SSO).

Les systèmes de gestion de l'identité fédérée pourraient fournir des capacités d'authentification et d'autorisation reconnues par-delà les frontières d'une organisation et d'un système. Cela présuppose la mise en place d'accords commerciaux et fiduciaires afin que l'identité d'un utilisateur chez un fournisseur soit reconnue par les autres fournisseurs (membres de la fédération). En général, un accord fiduciaire inclut également un accord contractuel sur la propriété des données, l'utilisation des informations d'identification personnelle (PII) et la conformité [UIT-T X.1242].

Le modèle de fédération est avantageux pour l'utilisateur, car un fournisseur de service d'identité offre habituellement une expérience d'authentification unique à un utilisateur. Cela réduit le nombre de justificatifs distincts qu'un utilisateur doit obtenir et maintenir. Dans ce modèle, les parties

utilisatrices membres de la fédération, ainsi que leurs utilisateurs, sont tributaires de la disponibilité d'un service donné du fournisseur IdSP et de sa volonté de rester dans la fédération.

Dans le modèle de la fédération, tout comme dans le modèle d'identité centralisé, l'authentification n'est pas mutualisée et présente les mêmes limites.

### 6.3 Modèle d'identité décentralisé

L'identité décentralisée pourrait être mise en œuvre au moyen de la technologie DLT ou d'autres technologies nouvelles fondées sur des normes telles que les déclarations vérifiables [b-W3C-1] et les identificateurs décentralisés (DID) [b-Sovrin], [b-W3C-1] et [b-W3C-2]. Un modèle d'identité décentralisé peut être construit au-dessus d'un registre distribué (DLT) et d'une relation entre un utilisateur et une organisation [b-Sovrin] et [b-W3C-17]. Dans ce modèle, l'utilisateur et l'organisation sont des homologues.

L'identité décentralisée permet aux utilisateurs de disposer du contrôle et de la propriété de leurs identités. Le degré de propriété peut varier selon le modèle décentralisé. Dans le modèle d'identité auto-souveraine (SSI), il est présumé que les entités sont capables d'avoir le contrôle de leur propre identité numérique.

La plupart des solutions d'identité actuelles offrent une prise en charge limitée du contrôle de l'identité, de la transparence et de la portabilité, étant donné que les fournisseurs de services d'identité dotés de systèmes propriétaires favorisent ce type de solutions. Un système d'identité respectant pleinement un modèle SSI pourrait voir le jour dans un proche avenir, mais cela n'exclut pas la nécessité d'en définir les principes fondateurs, comme indiqué aux § 6.3.1 et 6.3.2. L'utilisation de la technologie DLT pour la gestion de l'identité décentralisée est abordée plus avant au § 7.

#### 6.3.1 Identificateurs décentralisés

Les identificateurs décentralisés DID [b-W3C-2] sont un type d'identificateurs pour les systèmes d'identité vérifiables, décentralisés. Le format des DID leur permet d'être sous le contrôle du sujet du DID, ce qui les rend indépendants de tout registre centralisé, fournisseur d'identité, ou autorité de certification. Les DID sont des localisateurs uniformes de ressource (URL) qui relient un sujet de DID à des moyens d'interaction de confiance avec ce sujet. Les éléments standard d'un document DID (DDO) [b-W3C-2] comprennent:

1) un DID (pour l'auto-description);
2) un ensemble de clés publiques (pour la vérification);
3) un ensemble de protocoles d'authentification (pour l'authentification);
4) un ensemble de points d'extrémité de service (pour l'interaction);
5) un marqueur temporel (pour la chronologie d'audit);
6) une signature (pour l'intégrité).

Le déchiffrement d'un DID [b-W3C-2] donne un DDO, qui est un simple document décrivant comment utiliser ce DID spécifique. Chaque document DID contient au moins trois éléments: du matériel cryptographique, des suites d'authentification et des points d'extrémité de service. Le matériel cryptographique combiné aux suites d'authentification forment un ensemble de mécanismes pour authentifier un sujet de DID (qui est l'utilisateur lié au DDO). Les options d'authentification peuvent être par exemple des clés publiques et des protocoles d'authentification biométriques pseudonymes. Les points d'extrémité de service permettent des communications de confiance avec le sujet du DID.

Pour utiliser un DID [b-W3C-2] avec un registre distribué particulier, il est nécessaire de définir une méthode DID, en se basant par exemple sur la référence [b-RFC 8141]. Une méthode DID précise l'ensemble des règles qui décrivent la manière dont un DID est enregistré, rétabli, mis à jour et annulé sur un registre DLT spécifique. Tous les DID sont indiqués et rétablis sur un registre distribué.

L'utilisation d'un DID basé sur un registre DLT [b-W3C-2] réduit la dépendance vis-à-vis des registres centralisés pour les identificateurs ainsi que des autorités de certification centralisées pour la gestion des clés. Étant donné que les DID se trouvent sur un registre distribué, chaque entité peut être utilisée comme son propre domaine de confiance, créant ainsi une infrastructure de confiance décentralisée. Cela génère un relais d'interopérabilité entre les environnements centralisés, fédérés et décentralisés.

Le DID possède une paire de clés de chiffrement publique et privée [b-W3C-2]. La propriété d'un DID est établie par des algorithmes de chiffrement qui repose sur une clé privée, que le propriétaire du DID devrait être le seul à posséder. Les DID peuvent ainsi être publiés, échangés, consultés ou supprimés. Étant donné que chaque registre DLT a sa propre mise en œuvre de méthode DID, il existera, dans la pratique, différentes mises en œuvre pour les opérations de création, lecture, mise à jour et suppression (CRUD) pour le DID.

### 6.3.2 Justificatifs vérifiables

Les justificatifs vérifiables [b-W3C-1] résolvent le problème d'échange de justificatifs tels que les permis de conduire, les attestations de majorité ou d'âge, les preuves de formation et de qualification, les données de santé, par un réseau de communication en garantissant la vérification tout en préservant la protection des informations d'identification personnelle PII. Dans cette approche, les justificatifs se composent de déclarations appelées déclarations vérifiables. Les déclarations vérifiables [b-W3C-1] sont utiles lorsqu'une entité a besoin de prouver par exemple:

- un âge minimum requis;
- sa capacité à conduire un certain type de véhicule à moteur;
- son besoin d'un traitement particulier;
- sa formation et sa certification en tant qu'électricien;
- sa capacité à exercer la médecine par un diplôme professionnel;
- qu'elle est autorisée à voyager à l'international.

L'écosystème de justificatifs vérifiables se compose de quatre rôles primaires:

1) l'émetteur qui délivre les justificatifs vérifiables à propos d'un sujet spécifique;
2) le détenteur qui stocke les justificatifs pour le compte d'un sujet. Les détenteurs sont en général également le sujet d'un justificatif;
3) le vérificateur qui interroge un profil du sujet. Un profil contient un ensemble spécifique de justificatifs. Le vérificateur confirme que les justificatifs fournis dans le profil répondent à l'objectif;
4) le registre de l'identificateur qui est un mécanisme utilisé pour émettre des identificateurs pour les sujets.

Une déclaration [b-W3C-1] est une affirmation à propos d'un sujet, exprimée comme une relation sujet-propriété-valeur. Les déclarations peuvent être fusionnées pour représenter des graphiques d'information sur un sujet particulier.

Lorsqu'un émetteur envoie des données à un détenteur, il regroupe un ensemble de déclarations dans une structure de données appelée un justificatif et signe numériquement la structure de données [b-W3C-1]. Lorsqu'un vérificateur demande des données à un détenteur, le détenteur regroupe en général un ensemble de justificatifs dans une structure de données appelée un profil et signe numériquement la structure de données [b-W3C-1].

## 7 Identité décentralisée utilisant la technologie DLT

L'identité décentralisée peut être perçue comme une identité qui est ancrée par une technologie DLT. Dans cette approche, la preuve à apport nul de connaissance [b-W3C-1] peut relier des identités d'une

manière découvrable par tous. Une identité décentralisée permet à un utilisateur de prouver son identité une fois à une partie tierce de confiance et de stocker la preuve de son identificateur dans un registre distribué. Le registre distribué fait office de chambre forte de confiance pour protéger l'identité. La technologie des registres distribués offre notamment des services d'infrastructure d'identité prenant en charge les communications entre homologues, les services d'infrastructure de clé publique (PKI) basés sur la technologie DLT et les protocoles d'échange pour les déclarations vérifiables.

L'identité décentralisée permet aux utilisateurs d'accéder à des services de façon plus directe. Par exemple, un utilisateur interagit avec un fournisseur IdSP qui en retour utilise un registre DLT pour créer un DID utilisateur qui renvoie à un emplacement DLT que l'utilisateur peut utiliser. Cette étape est transparente pour l'utilisateur final. Elle équivaut à créer une paire de clés publique et privée pour l'utilisateur. La clé privée est stockée avec l'utilisateur sous la forme d'un porte-monnaie numérique. La clé publique correspondante est sauvegardée dans le registre DLT. La clé publique fait office d'identificateur du porte-monnaie (également connue comme l'identité utilisateur sur le registre DLT), elle est hachée et stockée de façon sécurisée dans un registre. Parmi les services offerts par la technologie DLT, les déclarations peuvent être émises et signées pour un utilisateur particulier par les émetteurs DLT et mises à la disposition de l'utilisateur. Ces déclarations peuvent être stockées dans le porte-monnaie de l'utilisateur.

Dans ce modèle, un utilisateur peut accéder à un service en présentant son identificateur à un fournisseur de service sous la forme d'un jeton. Le fournisseur de service vérifie l'identité en comparant les valeurs hachées de l'identificateur avec les enregistrements hachés stockés dans le registre DLT. Le fournisseur de services peut alors autoriser ou rejeter l'accès selon le résultat de la vérification.

### 7.1 Lancement du porte-monnaie

Le travail dans [b-Sovrin] et [b-W3C-1] donne un exemple d'interaction pour la prise en charge de service basé sur l'identité. Un utilisateur décide d'interagir en utilisant les services d'identité décentralisés d'un système d'identité de confiance basé sur la technologie DLT. À cet égard, la technologie DLT fournit des services pour permettre à l'utilisateur final d'établir un DID et une relation avec le registre. La création d'un DID pour l'utilisateur se conclut par la sauvegarde d'une adresse de registre pour cet utilisateur et la création de paires de clés publiques privées pour l'interaction avec l'utilisateur. Le registre peut également fournir des services qui peuvent être utilisés pour créer le document DID et établir les liens de documents requis, selon les spécifications de l'utilisateur. Le registre fournit des services d'identité centraux qui permettent aux services de découvrir comment interagir avec le porte-monnaie de l'utilisateur pour procéder à des demandes d'information au sujet de déclarations disponibles sous le contrôle de l'utilisateur.

La création d'un DID sur le registre induit la création d'un porte-monnaie que l'utilisateur utilise pour fournir des déclarations vérifiées aux parties utilisatrices (RP). Le porte-monnaie contient les clés privées de l'utilisateur, les clés publiques et d'autres profils d'identité tels que définis dans la méthode DID. Les techniques à apport nul de connaissance [b-Sovrin] garantissent que les déclarations peuvent être vérifiées de façon à préserver les informations d'identification personnelle et en conformité avec l'utilisation actuelle des justificatifs et documents papier classiques. Un utilisateur peut par exemple prouver son âge à un établissement avec un permis de conduire sans qu'il soit besoin pour l'autorité de délivrance du permis de conduire de participer à la transaction. Le porte-monnaie peut être un porte-monnaie virtuel dont une partie se trouve sur le dispositif mobile de l'utilisateur et l'autre partie dans le nuage. Cette configuration permet la création d'agents agissant pour le compte de l'utilisateur et exécutant des services sans qu'une implication directe de l'utilisateur ne soit nécessaire.

Les étapes suivantes sont essentielles pour le processus:

1) Registre DID: l'utilisateur télécharge le porte-monnaie associé au fournisseur de services DLT et enregistre son DID sur le registre. La technologie DLT génère la paire de clé publique privée associée au porte-monnaie d'identité. Une adresse est créée et sauvegardée sur le registre DLT dans le cadre du processus d'enregistrement.

2) Lancement de l'identité: pour qu'un registre DLT soit utilisé dans des systèmes d'identité décentralisés, on suppose l'existence d'un cadre de confiance qui définit une liste de services d'identité disponibles pour les participants. Partant de cette hypothèse, un utilisateur peut se fier à la disponibilité d'un émetteur (une partie de confiance) qui peut valider l'identité des utilisateurs. Au départ, les utilisateurs peuvent commencer avec des profils auto-déclarés. Les utilisateurs peuvent ensuite créer des déclarations initiales pour recueillir des déclarations complémentaires auprès de fournisseurs divers à ajouter dans leurs porte-monnaie et pour renforcer la validité de leur identité au sein du système. Chaque relation est protégée par un DID commun à l'émetteur, au détenteur (utilisateur) et au vérificateur.

3) Vérification: si un détenteur (utilisateur) souhaite avoir accès au service d'une partie utilisatrice, cette partie utilisatrice (vérificateur) demandera à l'utilisateur d'autoriser un accès à des déclarations disponibles dans son porte-monnaie. Le vérificateur procèdera à la consultation avec la technologie DLT pour valider les déclarations signées en utilisant les clés publiques correspondant au DID défini dans la transaction. Le système admet l'hypothèse que le porte-monnaie est la source de vérité en termes de connaissance des clés privées de l'utilisateur. Le système admet l'hypothèse qu'une authentification adaptée a eu lieu pour garantir que le propriétaire légitime du porte-monnaie est bien l'entité à l'origine de la transaction.

4) Validation de la déclaration: la partie utilisatrice utilise les déclarations fournies par le porte-monnaie pour vérifier l'identité et les attributs de l'utilisateur en utilisant la signature PKI basée sur la technologie DLT et les techniques de validation hachée.

5) Autorisation: la partie utilisatrice détermine à quels services elle donne accès en fonction du résultat des vérifications d'identité.

### 7.2 Résolution et authentification DID

Le concept DID [b-W3C-2] peut faciliter la création d'un interpréteur universel [b-DIF] pour tout DID. L'interpréteur universel peut participer à une couche d'authentification DID interopérable. L'authentification DID permet à un propriétaire d'identité de prendre le contrôle d'un DID pendant son interaction avec une partie utilisatrice. Cela nécessite l'exécution des étapes suivantes par la partie utilisatrice:

1) La partie utilisatrice traduit le DID du propriétaire d'identité sur un registre DLT en un document DID.

2) La partie utilisatrice essaie d'authentifier le propriétaire d'identité en utilisant le ou les objets d'authentification trouvés dans le document DID sur le registre DLT.

3) Le ou les objets d'authentification peuvent comprendre un objet de clé publique ou y faire référence, dans les cas où la preuve du propriétaire d'identité est établie sous forme de signature chiffrée.

### 7.3 Avantages de l'utilisation de la technologie DLT pour la gestion d'identité et d'accès décentralisée (DIdAm)

L'utilisation de la technologie DLT comme cadre de confiance pour les systèmes d'identité décentralisés ouvre la voie aux fournisseurs pour concevoir des cadres qui permettraient aux fournisseurs de faire office de couche de représentation abstraite intergicielle entre l'utilisateur et les différents registres. Ces interactions nécessitent des systèmes de gestion d'identité et d'accès classiques pour définir un cadre adapté à la prise en charge les systèmes décentralisés. Dans les faits, la fusion entre les systèmes centralisés et décentralisés peut être considérée comme un système de

gestion d'identité décentralisé (DIdAm) [b-Angelov et al.]. À cet égard, un système DIdAm [b-Angelov et al.] est un ensemble composé de systèmes capables d'interagir avec plusieurs registres DLT prenant en charge des modèles d'identité décentralisés basés sur des DID. C'est ce que décrit la Figure 1 ci-dessous.

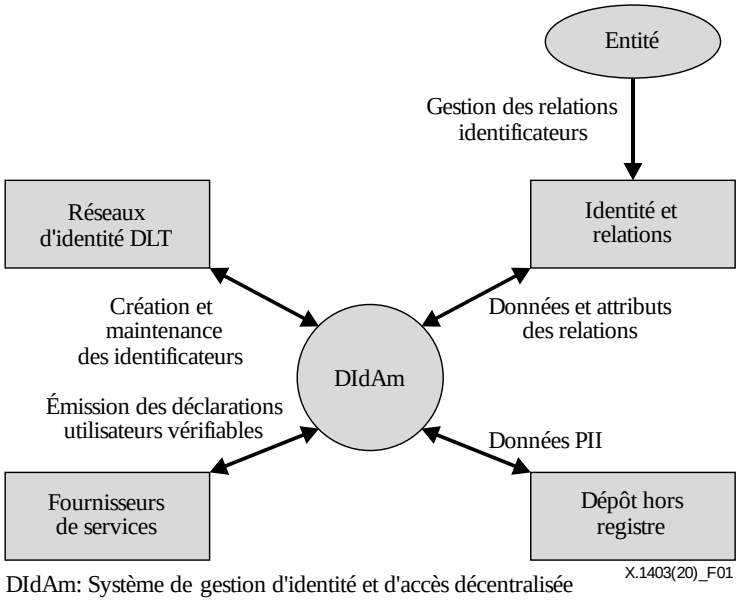


**Figure 1 – Cadre DIdAm**

Un système DIdAm utilisant la technologie DLT comprend:

1) le propriétaire d'identité décentralisé: c'est une entité qui gère ses identités décentralisées en utilisant des services offerts par un DIdAm au travers de plusieurs registres;

2) des fournisseurs de services (SP): les émetteurs qui proposent des services à des propriétaires d'identité (identité d'amorçage). Par exemple, des agences gouvernementales telles que l'autorité délivrant les permis de conduire ou des entreprises privées telles que des établissements financiers;

3) un dépôt d'identité hors registre: il s'agit d'une base de données dans laquelle sont stockés les attributs d'identité, les déclarations et les informations générales de l'utilisateur. L'utilisateur contrôle l'emplacement où devraient être stockées les données. Ce sont généralement des données PII sensibles, étant donné leur caractère personnel, qui devraient être stockées hors registre. Le dépôt devrait donner la capacité de lecture/écriture des données à la convenance de l'utilisateur;

4) les systèmes d'identité basés sur la technologie DLT peuvent être conçus comme des systèmes d'identité distincts avec différentes limites d'autorisation et clés chiffrées. Par conséquent, le système de gestion DIdAm doit faciliter les interactions au sein des registres pour le compte de l'utilisateur.

Les services de gestion DIdAm peuvent être fournis en interne par l'entreprise ou par un tiers qui joue le rôle de fournisseur de ces services.

### 7.3.1 Prise en charge des identités décentralisées dans les différents registres DLT

La prise en charge des identités décentralisées grâce à l'utilisation de DID dans différents registres DLT fait appel à de nombreuses spécifications d'interface [b-Angelov et al.]. La difficulté vient des changements de spécifications du cadre de confiance, par exemple le type de registre DLT, public ou privé. La gestion DIdAm devrait être en mesure de prendre en charge l'utilisateur indépendamment des préférences de l'utilisateur quant au type d'équipement de télécommunication ou de réseau d'accès

utilisé. La Figure 1 présente la gestion DIdAm sous forme d'interface unifiée vis-à-vis du propriétaire d'identité, capable d'opérer sur plusieurs registres.

La gestion DIdAm [b-Angelov et al.] fait office de couche de représentation abstraite pour l'utilisateur final. Cela permet à l'utilisateur d'interagir avec plusieurs registres DLT tout en utilisant une seule interface virtuelle. La gestion DIdAm fait également office de couche de représentation abstraite pour l'entreprise sachant que les systèmes de gestion d'identité traditionnels peuvent interagir avec elle, apportant un appui aux fonctions internes de la gestion d'identité centralisée. Un avantage de cette représentation abstraite pourrait être la capacité d'un utilisateur à gérer des identités sur n'importe quel nombre de registres. Ce qui permet à l'utilisateur de créer des relations avec des fournisseurs et d'avoir un meilleur contrôle de son identité.

### 7.3.2 Prise en charge des services d'identité

Dans les systèmes IdAm classiques, le fournisseur de service d'identité est capable d'attester l'identité d'un utilisateur à une partie utilisatrice. La gestion DIdAm [b-Angelov et al.] devrait être capable de prendre en charge ce rôle, notamment pour être compatible avec les systèmes traditionnels antérieurs. Les mesures suivantes permettent la prise en charge du besoin d'attestation:

1) La gestion DIdAm devrait agir comme un partenaire de confiance. Elle devrait garantir que le propriétaire d'identité obtienne des assertions exactes et valides par de bonnes procédures de déclarations vérifiables pour les émetteurs.
2) Réduire les difficultés liées aux vérifications d'identité pour les utilisateurs. Généralement, un utilisateur devra passer par une authentification d'identité pour chaque émetteur. Une gestion DIdAm bien conçue peut aider l'utilisateur à remédier à cette contrainte en faisant office de participant de confiance actif dans cette interaction.
3) Validation des données en temps réel. Les données inexactes posent un problème dans les systèmes traditionnels, lequel problème peut être résolu par la gestion DIdAm au travers d'une offre de services aidant les parties utilisatrices à vérifier que les attributs d'utilisateur ne sont pas expirés.
4) Gestion des consentements. Le consentement fait partie intégrante de la conformité. La gestion DIdAm peut proposer des services aux utilisateurs et aux parties utilisatrices pour garantir le respect du consentement.

### 7.3.3 Gestion du porte-clés

Le terme porte-clés fait référence à la sécurisation de la sauvegarde des clés privées associées à un porte-monnaie sur le dispositif de l'utilisateur. Il existe une relation univoque directe entre le DID, le justificatif vérifiable et le fournisseur de services. Le dispositif peut être mobile ou basé sur un navigateur. Par conséquent, dans le présent modèle de sécurité, l'accès aux clés privées est utilisé pour la validation de l'identité de l'utilisateur. La tâche de protection des paires de clés est essentielle pour prévenir les attaques liées à la fraude d'identité. Le traitement de plusieurs DID sur de nombreux registres DLT confronte les utilisateurs à la nécessité de protéger un ensemble de clés privées utilisées pour déverrouiller leur identité dans l'ensemble du périmètre nécessitant une identification.

Le porte-clé est la structure au sein de laquelle la clé privée correspondant aux DID de l'utilisateur est stockée de façon sécurisée. Il s'agit d'une structure appartenant au propriétaire d'identité et qui commande les clés privées, ce qui équivaut à posséder les DID. Une gestion DIdAm devrait être capable de gérer le porte-monnaie pour le compte de l'utilisateur. Notamment:

1) l'utilisateur devrait être capable d'utiliser la fonction de porte-monnaie et de stockage tout en restant actif dans le domaine de la gestion DIdAm;
2) la gestion des clés devrait être sous le contrôle de l'utilisateur;
3) l'accès au porte-clé devrait être géré et auditable;

4) les services permettant à l'utilisateur de sauvegarder et de restaurer le porte-monnaie peuvent être proposés par le DIdAm.

## 8 Lignes directrices sur la sécurité relatives à l'utilisation de la technologie DLT pour la gestion DIdAm

L'identité décentralisée résout certains problèmes liés aux modèles d'identité centralisés et fédérés. La technologie des registres distribués est vulnérable aux risques de cybersécurité. Les risques de sécurité incluent les risques liés à des erreurs humaines telles que les erreurs de codage de logiciel.

En général, les DID utilisateur ne devraient pas être publiés sur un registre "sans permission", même si dans certains cas, il pourrait être nécessaire d'avoir un identifiant unique mis à la disposition de tous ses utilisateurs. Toutefois, les données aidant les utilisateurs à se fier au registre telles que les clés publiques IdSP, les listes de révocation et les données renforçant l'interopérabilité, telles que les schémas à justificatifs variables, peuvent être rendues publiques sur les registres.

Ce paragraphe traite des avantages et des défis de sécurité, ainsi que des risques de sécurité pour les modèles d'identité décentralisés.

### 8.1 Considérations relatives à la sécurité des registres distribués

Il existe deux grands types de registres distribués, classés en deux catégories: les registres "sans permission" et les registres "de permission". Les registres "sans permission" autorisent n'importe quelle entité à accéder, consulter, proposer de nouvelles données ou à valider des données existantes sur le registre, à condition que celle-ci se conforme aux protocoles définis du registre. Le registre garantit la confidentialité, l'intégrité, la disponibilité et la cohérence des données avec les protocoles qui ont fait consensus pour créer un climat de confiance entre les participants qui pourraient ne pas se faire confiance entre eux. En général, les registres "sans permission" fonctionnent sans autorité centrale.

Un registre de permission est un système composé de parties de confiance à qui des droits d'utilisation sont confiés selon les besoins de leur rôle respectif dans le cadre de confiance. Selon ce modèle, des participants choisis peuvent échanger des données sur le registre. Selon les accords fiduciaires, certains registres peuvent autoriser un accès libre, en mode lecture seule.

Le registre "sans permission" garantit la confiance à travers les protocoles qui ont fait consensus mais qui sont gourmands en termes de calculs et cela a un impact direct sur la qualité du débit et du fonctionnement du système d'identité qui les exploite. À l'inverse, le registre de permission se fonde sur la confiance entre les créateurs du registre pour garantir la sécurité des données de ce dernier, notamment les données d'identité. Les registres de permission sont généralement plus rapides et plus économiques que les registres "sans permission".

### 8.2 Avantages de l'utilisation du DID pour la technologie DLT

L'identité décentralisée présente les avantages suivants:

1) Portabilité de l'identité: le DID décentralisé garantit que les personnes ont le contrôle de leurs identités numériques. Il supprime la dépendance vis-à-vis d'un fournisseur IdSP centralisé. En théorie, les personnes peuvent posséder, contrôler et gérer leurs propres identificateurs et leurs relations.
2) Promotion des services d'identité basés sur les relations: le DID permet aux entités d'établir des identificateurs numériques pour presque toutes les relations. Les DID pseudonymes opérant par paires préservent les informations d'identification personnelle.
3) Réduction du risque de sécurité: les DID nécessitent que les propriétaires d'un identificateur apportent la preuve de la propriété en démontrant la connaissance de la clé privée associée à la clé publique correspondante. La validation de la déclaration est vérifiée de façon

dynamique en temps réel sur le registre DLT. La validation peut s'effectuer sans recours à des serveurs centralisés ce qui réduit la surface vulnérable.

4) Répartition des coûts: la validation d'identité sur un registre DLT bénéficie de la capacité d'utiliser le DID pour réutiliser la confirmation d'identité entre les participants du registre DLT. Cela réduit les coûts et renforce la sécurité.

5) PII par conception: les services DID souverains décentralisés répartissent le risque résultant de l'utilisation de banques de données centrales pour stocker des informations utilisateurs et cela augmente par là-même la difficulté pour les pirates.

6) Partage consenti et suivi des données personnelles: le DID donne la capacité de partager des données entre utilisateurs et fournisseurs sur la base de politiques convenues au préalable, ce qui améliore la capacité de l'utilisateur à protéger ses données.

7) Fédération dynamique et plus forte: l'utilisation de DID dans un registre DLT augmente la confiance de toutes les organisations participant à l'écosystème. Les participants peuvent se concentrer sur la fourniture de services plutôt que de se concentrer sur les détails de la fédération et la façon de la mettre en place.

8) Tolérance aux pannes: la nature décentralisée de la technologie DLT donne un niveau de tolérance aux pannes et de résilience d'infrastructure.

### 8.3 Menaces et vulnérabilités

Les registres distribués ont hérité de capacités qui atténuent les risques en termes de cybersécurité sur les systèmes des technologies de l'information et de la communication. Ces fonctions de sécurité améliorée présentent notamment:

1) une résilience du système accrue: l'architecture distribuée d'un registre DLT lui évite de devenir un point de défaillance isolé;

2) une meilleure robustesse: les mécanismes de consensus améliorent l'intégrité générale des registres distribués, car le consensus entre les participants est nécessaire avant d'accepter toute nouvelle information sur le registre;

3) plus de transparence: il est plus difficile pour les logiciels malveillants d'opérer au sein du registre distribué étant donné que le système possède plusieurs couches distinctes de sécurité au niveau de l'infrastructure du registre.

Les systèmes d'identité décentralisés conçus avec la technologie DLT hériteront des risques de sécurité propres à cette technologie. En outre, il existe des risques supplémentaires liés à l'utilisation de la technologie DLT pour la gestion d'identité.

#### 8.3.1 Gestion des données d'identité

CRUD est l'acronyme anglais pour créer, lire, mettre à jour et supprimer *(create – read – update – delete)*. Il s'agit des opérations de base des banques de données de stockage. Dans la technologie DLT, en particulier avec la blockchain de permission, les entités de mise en œuvre ne peuvent pas supprimer de transactions écrites sur une blockchain. Même la mise à jour de transactions existantes ne peut être effectuée, dans la mesure où celles-ci sont immuables. Par conséquent, les opérations "CRUD" ne peuvent pas être considérées comme une opération normale de traitement des données utilisateurs.

Les opérations sur la blockchain peuvent plutôt être décrites avec l'acronyme anglais CRAB pour: créer, extraire, adjoindre et graver *(create – retrieve – append – burn)*. L'ajout, qui remplace la mise à jour, signifie que lors de la mise en œuvre, il est seulement possible d'adjoindre de nouvelles transactions à la technologie de blockchain, modifiant ainsi "l'état du monde" (somme de tous les événements/transactions passés à ce jour). L'opération de gravage dans CRAB signifie que vous jetez les clés de chiffrement, ce qui signifie que vous n'êtes pas en mesure d'adjoindre de nouvelles transactions ni de procéder à une modification ultérieure de l'état du registre de l'infrastructure.

Il est par conséquent important d'être très prudent avec l'écriture de données personnelles sur un registre DLT ou une blockchain dans la mesure où ces données ne peuvent être ni retirées, ni oubliées à l'avenir. À cet égard, il vaut mieux écrire les données en dehors de la chaîne avec des pointeurs dans le registre DLT pointant vers les données situées à l'extérieur. Toutefois, stocker des données en dehors du registre présente également des inconvénients. Notamment:

- l'avantage de transparence est réduit dans la mesure où les utilisateurs ne sauront pas s'ils ne sont pas autorisés à accéder aux données hors registre;
- l'avantage de la propriété des données avec la blockchain est réduit, car une fois que les données sont hors registre, elles peuvent devenir la propriété de n'importe quelle entité qui peut y accéder.

### 8.3.2 Possibilité de relier la clé DID

Les DID peuvent potentiellement être corrélés. Cela peut se produire si le même DID est utilisé avec plus d'une relation. Les registres DLT peuvent atténuer ce risque en utilisant des DID uniques par paire pour des relations. Cela signifie que chaque paire de DID utilisés est différente pour chaque relation. Dans ce scénario, chaque DID fait office de pseudonyme [b-W3C-2]. Un DID pseudonyme doit seulement être partagé avec plus d'une partie, lorsque le sujet du DID autorise explicitement la corrélation en ces parties.

Il convient de noter par mesure de précaution que même les DID pseudonymes peuvent être corrélés [b-W3C-2] si les données des documents DID correspondants peuvent être corrélées. Par exemple, l'utilisation de noms de points d'extrémité de service communs dans plusieurs documents DID peut servir à relier des informations à propos du même DID. Par conséquent, le document DID pour un DID pseudonyme doit également utiliser des clés publiques uniques par paires.

### 8.3.3 Protection de clé DID

La gestion des clés privées est importante. Si une clé maître est stockée dans un emplacement non sécurisé, même sur un dispositif isolé, un vol d'identité est probable. L'utilisation d'équipements de stockage sécurisé sur les dispositifs devrait être obligatoire.

### 8.3.4 Techniques de préservation des PII

Il est recommandé de ne pas stocker d'informations sensibles sur le registre. Avec l'avènement de l'informatique quantique, il est certain que n'importe quelle technique de cryptage dans les deux sens finira par être contournée avec le temps, l'objectif étant de ne jamais stocker d'information sensible sur le registre.

Bien que les hachures soient des fonctions unidirectionnelles, elles peuvent être potentiellement sensibles dans la mesure où les pirates disposent d'un temps illimité pour attaquer par force brute le résumé. Pour cette raison, les hachures ne devraient pas être stockées sur le registre.

Plutôt que de sauvegarder des données brutes telles qu'une date de naissance sur le registre, des réponses à des questions établissant qu'une personne a plus de 21 ans par exemple pourraient être sauvegardées dans un contrat intelligent sur un registre. Elles pourraient être considérées comme une déclaration conforme à une exigence.

Il est recommandé de ne stocker que des hachures de données privées ou sensibles sur le DLT. Les données PII ne devraient pas être stockées sur le registre, même en cas de chiffrement. Les données sensibles devraient être stockées hors registre et devraient être échangées entre des entités approuvées qui ont besoin de consommer ces données. Cette approche réduit le risque qu'une violation du registre DLT n'induise la perte de données sensibles. Il faudrait utiliser une technologie entre homologues sécurisée pour les échanges de données prenant en charge l'accès hors registre. Il faudrait également utiliser des techniques de stockage des données hors registre appropriées incluant des plans d'archivage et de reprise des données. Par exemple, si un propriétaire d'identité affirme être un fournisseur de garantie homologué, cette déclaration peut être vérifiée par une entité jouant le rôle du

fournisseur de confiance dans le système d'identité décentralisé, et le justificatif est stocké dans le registre DLT sous une forme hachurée. Le justificatif peut être la hachure de la déclaration portant la signature numérique du déclarant. La sécurité du dépôt hors registre devrait être garantie.

### 8.3.5 Verrouillage du vendeur

Les registres peuvent être standardisés, mais les composants logiciels sont propres à une solution donnée et pourraient s'avérer exclusifs et non-interopérables.

### 8.3.6 Attaques basées sur l'identité

Un registre distribué est vulnérable aux attaques basées sur l'identité à l'instar de celles ciblant l'infrastructure des technologies de l'information, telles que l'usurpation d'identité et les attaques Sybil. Des individus malveillants peuvent lancer de telles attaques pour s'emparer de la plupart des nœuds dans un registre. S'ils réussissent, ces pirates peuvent fragiliser la validation consensuelle et les protections de l'architecture distribuée d'un registre. Le risque peut être atténué grâce à l'utilisation de solutions d'authentification concrètes pour des services de répertoire en nuage.

### 8.3.7 Effets des réseaux de communication

La structure distribuée de la technologie DLT peut poser des problèmes en termes d'exploitation lorsque plusieurs acteurs sont impliqués, chacun ayant ses propres solutions pour protéger son infrastructure de communication. Cette configuration pose des défis en matière de gestion des identités, de contrôle d'accès, de configuration de la sécurité, de stockage et de gestion de clés PKI.

Les opérations DLT nécessitent des nœuds d'exploitation utilisant différentes topologies de réseau, codes logiciels et protocoles, qui peuvent s'avérer vulnérables aux menaces de sécurité. Les répercussions de ces menaces varient selon la nature du registre DLT (privé ou public). Les systèmes de gestion des identités et les données d'identité sont vulnérables aux attaques du réseau de communication ciblant les registres DLT. Les concepteurs des systèmes de gestion des identités devraient tenir compte des questions ci-après concernant le réseau de communication:

1) Quelles seraient les répercussions sur les données d'identité en cas d'échec de l'algorithme de consensus de la technologie DLT?
2) Comment traiter les collisions avec la technologie DLT ou la blockchain?
3) Quel est le plan de reprise après sinistre pour les données d'identité?
4) Quelles sont les menaces pesant sur les données d'identité si un petit groupe de participants prend le contrôle des mécanismes de consensus de la technologie DLT?

### 8.3.8 Chiffrement des données d'identité

Les données d'identité stockées hors registre sont considérées comme confidentielles et privées pour le propriétaire d'identité. L'utilisateur devrait être en mesure d'obtenir de l'aide du registre pour le cryptage des données en masse ou durant la transmission, notamment lors du partage des données entre les différents fournisseurs.

### 8.3.9 Procédure de sauvegarde

Il existe des risques pour l'utilisateur en matière de protection de ses dispositifs et contenus en ce qui concerne les déclarations vérifiables, les clés privées ou les données personnelles.

Il en résulte donc un besoin de procédure adaptée pour la récupération et la restauration des données pour le porte-monnaie de l'utilisateur.

En outre, l'utilisateur aura besoin de l'assurance que ses données sont protégées et sauvegardées sur le registre. Des techniques garantissant qu'il n'y a pas de corruption ni de perte de données devraient être mises à la disposition de l'utilisateur final sous forme de services.

### 8.3.10 Contrats intelligents

L'utilisation de contrats intelligents peut être requise dans la mise en œuvre des systèmes d'identité décentralisés. Les contrats intelligents sont établis par des développeurs utilisant des langages de programmation informatique. Ces programmes sont susceptibles de contenir des erreurs de développement et de programmation notamment du fait de la complexité croissante des contrats intelligents. L'incertitude quant à l'exactitude des contrats intelligents rend nécessaire le développement d'un cadre de gouvernance pour garantir que les systèmes d'identité décentralisés ont des processus et des procédures propres pour faire face à toute contrainte liée à l'inexactitude de contrats intelligents, que celle-ci soit de nature intentionnelle ou non.

### 8.3.11 Gestion des certificats DLT

Les systèmes de gestion des identités comprennent la gestion du cycle de vie des identités qui englobe à son tour les tâches de vérification d'identité. Parmi les tâches liées à la gestion des identités figurent notamment la création, l'émission, le stockage, l'annulation et le remplacement des justificatifs et la détection de fraude.

L'utilisation de certificats dans les registres pose des défis uniques aux professionnels de la sécurité. Dans les systèmes d'identité décentralisés, le prix à payer pour la perte ou l'égarement de clés privées est plus élevé que pour des systèmes d'accès classiques. Par exemple, la perte des clés privées d'un porte-monnaie d'utilisateur entraîne la désactivation définitive de l'accès de l'utilisateur au réseau DLT. Le dommage peut être plus grand encore en cas de vol, car prouver la possession de clés privées équivaut à identifier le voleur. La difficulté des mécanismes de correction dépend également de la nature du DLT. Il est plus simple de traiter ces questions avec des registres privés comparativement aux registres "sans permission" qui requièrent des consensus sur des transactions.

Ces questions devraient être inclues dans la conception des systèmes de gouvernance des registres DLT car il n'existe pas d'autorité centrale pour lutter contre la fraude ou répondre aux difficultés techniques. Cela nécessite un cadre de gouvernance fiable pour garantir que tous les stades d'un cycle de vie de l'identité sont couverts dès le début et que des procédures appropriées sont adoptées au préalable par les participants DLT pour la prise en charge des services de rétablissement de l'identité. Sont concernées par exemple les questions suivantes: Comme le cycle de vie des clés est-il géré? Quelles sont les parties d'un bloc de charge utile qui sont chiffrées? Comment les clés sont-elles annulées? Comment les clés privées sont-elles protégées et rétablies? Que se passe-t-il en cas de détection de fraude?

# Bibliographie


[b-RFC 8141] RFC 8141, *Uniform Resource Names (URNs)*, avril 2017

[b-Angelov et al.] Angel Angelov, Mihail Milkov, Markus Sørensen *Decentralized Identity Management System for Self-Sovereign Identity* https://projekter.aau.dk/projekter/files/281068659/Master_Thesis_ICTE4SER4.2.pdf

[b-Baars] Djuri Baars, *Towards Self-Sovereign Identity using Blockchain Technology*; https://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf

[b-Blog] Blockchain platforms, https://medium.com/blockchain-blog/17-blockchain-platforms-a-brief-introduction-e07273185a0b

[b-DIF] Decentralized Identity Foundation (DIF) https://identity.foundation/#wgs

[b-Gartner] Gartner, Blockchain, *Evolving Decentralized Identity Design*, publié le 1er décembre 2017 – ID G00324208, par l'analyste Homan Farahmand.

[b-Sovrin] Sovrin Foundation, https://sovrin.org/

[b-W3C-1] W3C, *Verifiable Credentials Data Model 1.0 Expressing verifiable information on the Web*, https://www.w3.org/TR/2019/CR-vc-data-model-20190725/

[b-W3C-2] W3C, *Decentralized Identifiers (DIDs) v0.13 Data Model and Syntaxes*, août 2019, https://w3c-ccg.github.io/did-spec/

## SÉRIES DES RECOMMANDATIONS UIT-T

| | |
|---|---|
| Série A | Organisation du travail de l'UIT-T |
| Série D | Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC |
| Série E | Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains |
| Série F | Services de télécommunication non téléphoniques |
| Série G | Systèmes et supports de transmission, systèmes et réseaux numériques |
| Série H | Systèmes audiovisuels et multimédias |
| Série I | Réseau numérique à intégration de services |
| Série J | Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias |
| Série K | Protection contre les perturbations |
| Série L | Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures |
| Série M | Gestion des télécommunications y compris le RGT et maintenance des réseaux |
| Série N | Maintenance: circuits internationaux de transmission radiophonique et télévisuelle |
| Série O | Spécifications des appareils de mesure |
| Série P | Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux |
| Série Q | Commutation et signalisation et mesures et tests associés |
| Série R | Transmission télégraphique |
| Série S | Équipements terminaux de télégraphie |
| Série T | Terminaux des services télématiques |
| Série U | Commutation télégraphique |
| Série V | Communications de données sur le réseau téléphonique |
| **Série X** | **Réseaux de données, communication entre systèmes ouverts et sécurité** |
| Série Y | Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes |
| Série Z | Langages et aspects généraux logiciels des systèmes de télécommunication |

Imprimé en Suisse
Genève, 2021