[FR] Decentralized Identifiers (DIDs)

Rappels Identity and Access Management (IAM)

Il existe actuellement 3 grandes formes de Gestion d'Identité : le modèle dit en **silo**, le modèle **fédéré** et le modèle **user-centric.**

Le premier est le plus ancien, il s'agit du format classique où chaque organisation, entreprise, site web, etc accorde un accès à l'utilisateur après que celui-ci est fourni les informations demandées. Dans cette situation l'utilisateur se retrouve très vite avec énormément d'identités éparpillées et il est très difficile voir impossible de tout gérer. De plus, il arrive régulièrement qu'une trop grande quantité d'informations soit fournie (envoyer une copie de sa carte d'identité alors que seuls le nom et la date de naissance sont nécessaires). Dans le cadre du RGPD ce modèle n'est pas du tout recommandé.

Le deuxième modèle est l'un des plus répandus. Il consiste à "rassembler" des organisations souhaitant collaborer afin de mettre en place un système d'authentification unique. Il faut dans un premier temps s'authentifier auprès d'un tiers de confiance, qui va ensuite s'occuper de nous authentifier auprès des organismes affiliés.
C'est, par exemple, le modèle que l'on retrouve chez Microsoft : nous créons un "compte Microsoft" qui va servir de carte d'identité sur tous le réseau Microsoft. Ainsi, il suffit de s'authentifier une seule fois sur un service Microsoft pour ensuite être automatiquement authentifié lorsque l'on souhaite accéder à un service d'une organisation appartenant au réseau. Pour ce faire, la composante **Single Sign-On (SSO)** est utilisée. Il s'agit du mécanisme permettant la mise en place de l'authentification unique au sein de toute la fédération d'identités. La mise en place d'une fédération d'identités nécessite que les différents partis se mettent d'accord sur les informations nécessaires à l'identification et l'authentification, se mettent d'accord sur le format des données, etc. Dans cette optique, le protocole **SAML** est très couramment utilisé.

Le dernier modèle est celui qui permet de s'authentifier auprès de différents organismes en passant par un tiers de confiance sans qu'il n'y ait d'affiliation entre eux. C'est la situation que l'on retrouve lorsque l'on veut s'authentifier avec Facebook, Google, etc sur d'autres sites. L'inconvénient de ce modèle est que ces tiers de confiance sont garants de toute notre identité numérique et se retrouve avec beaucoup trop de pouvoir, ce qui peut vite poser problème et n'est pas compatible avec la vision du RGPD.

Depuis quelques temps un nouveau modèle est en train de se développer : l'identité auto-souveraine (**Self-Sovereign Identity, SSI**). Dans ce modèle, l'utilisateur est maître de sa propre identité numérique. Le principe est de se créer un portefeuille d'informations permettant de nous identifier (par exemple nom, prénom, date de naissance, photo d'identité, etc). Une fois ces informations choisies, nous pouvons les envoyer à une autorité compétente qui va les valider et nous fournir un certificat pour chacune d'elle. A partir de là, lorsqu'un fournisseur de service souhaitera vérifier notre identité, nous pourrons lui fournir uniquement les informations nécessaires sans avoir à en donner plus (il n'est pas utile d'envoyer sa carte d'identité avec toutes les informations qu'elle contient si seul le nom est requis).

Ce modèle se base principalement sur la **blockchain** pour le stockage des informations et ceci apporte plusieurs avantages. L'utilisateur étant maître de ses données, elle ne peuvent pas être utilisées sans son consentement. C'est lui qui accorde explicitement l'accès en lecture à ses données, et il est en mesure de le révoquer quand il le souhaite. Cela implique aussi que les entreprises n'ont plus besoin d'enregistrer les données, celles-ci étant accessible en lecture. Enfin, le fonctionnement de la blockchain permet une traçabilité complète des données et empêche ainsi toute falsification. Du point de vue du RGPD, ce modèle semble être le plus adapté en mettant l'utilisateur au centre et en retirant la possession et le contrôle des informations aux entreprises.

Présentation des Decentralized IDs

Concept général

Les Decentralized IDs (ou DIDs) sont une solution d'identification reposant sur la blockchain et permettant aux utilisateurs de s'identifier eux mêmes. Il s'agit d'une solution appartenant au concept de **Self Sovereign Identity (SSI)**.

Un utilisateur est en mesure de créer un nouveau DID à n'importe quel moment et pour n'importe quelle raison. Ce dernier est composé d'un identifiant unique et d'un document permettant de le décrire. L'identifiant est de la forme "did:method:123456789abcdefghi" (qui reprend la structure des URNs) tandis que le document est une structure de données en JSON-LD et est stocké de manière à être toujours accessible. Les DIDs sont vérifiables par cryptographie afin d'assurer leur authenticité et vérifier leur provenance.

Format DID - https://w3c-ccg.github.io/did-primer/#diddocuments

En plus de contenir un DID, le document peut contenir d'autres paramètres permettant de valider son authenticité tels que :

- Une date de création
- Une preuve cryptographique de sa validité
- Une liste de clés publiques
- Une liste de services où le DID peut être utilisé
- Des extensions

Voici un exemple de document provenant du W3C :

DID Document: https://www.w3.org/TR/did-core/#example-2-minimal-self-managed-did-document

EXAMPLE 2: Minimal self-managed DID document

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // used to authenticate as did:...:1fgh1
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }],
  "service": [{
    // used to retrieve Verifiable Credentials associated with the DID
    "id": "did:example:123456789abcdefghi#vcs",
    "type": "VerifiableCredentialService",
    "serviceEndpoint": "https://example.com/vc/"
  }]
}
```

On peut constater qu'il n'y a pas d'informations personnelles dans ce document. En effet, les DIDs n'ont pas pour objectif de transmettre des informations, mais de certifier la validités des informations fournies par d'autres documents, tels que les **Verifiable Credentials**. Les DIDs ont seulement une fonction de signatures. Les Verifiable Credentials ne seront pas abordés dans ce document car ils sont de la problématique et je pars du principe que le sujet est déjà connu du lecteur.

Dans l'exemple de format au dessus, le paramètre "method" est spécifié. Il s'agit de la solution de blockchain choisie pour enregistrer le DID. Parmi toute les méthodes, nous retrouvons le Bitcoin, l'Ethereum , etc. Au total, 9 technologies de blockchain sont disponibles. Ainsi, en connaissant la technologie utilisée il sera possible de retrouver le document associé au DID.

DIDAuth

Pour s'assurer que l'utilisateur qui envoie le DID en est bien le propriétaire légitime, la solution DIDAuth a été mise en place. Il ne s'agit ni plus ni moins que d'une technique de challenge/réponse. Le service demandant le DID envoie un challenge aléatoire que l'utilisateur va signer avec sa clé privée. Il va ensuite renvoyer le challenge, la signature et le DID.

trustspring2018/blob/master/final-documents/did-auth.pdf

La présentation haut niveau des DIDs terminée, nous pouvons maintenant passer à la seconde partie où nous allons étudier les arguments en faveur et en défaveur de cette nouvelle technologie.

Réflexion autour des DIDs

Cette nouvelle technologie semble vouloir répondre à certaines problématiques, mais quelles sont elles ? Et qui seront les différents acteurs et bénéficiaires de cette nouvelle technologie ?

Il est d'abord important de se demander qui seront les acteurs autour des DIDs. Comme dit précédemment, les DIDs sont une solution de signature numérique qu'il est intéressant de coupler au système des Verifiable Credentials. Les acteurs des DIDs sont donc les mêmes que pour les VCs. Nous allons retrouver : les utilisateurs, les Service Providers, les Claims Issuers et les fournisseurs de technologie.

- Utilisateur : le possesseur de DIDs et le sujet des Verifiable Credentials
- Service Provider : le site, l'application, l'entreprise, etc, qui a besoin de VCs pour fournir un service
- Claims Issuers : le gouvernement, une administration, ou autre, capable de fournir des VCs aux utilisateurs
- Les fournisseurs de technologies : les organismes en mesure de fournir la technologie nécessaire pour la mise en place des DIDs (la blockchain, etc) et de mettre en lien les différents acteurs

Les différents acteurs étant fixés, nous pouvons analyser ce que les DIDs peuvent leur apporter.

Utilisateurs

L'intérêt le plus visible et "évident" est le fait de redonner le contrôle à l'utilisateur grâce à la blockchain. En effet, il n' y a maintenant plus besoin de passer par un service tiers centralisant toutes les informations. L'utilisateur est en mesure de fournir ses DIDs et les conserve lui même sans risque que les informations soient révoquées par un tiers.

Cela limite non seulement le risque que l'autorité possédant les informations disparaissent, et les informations avec, mais aussi le pouvoir que les fournisseurs d'identité comme Facebook, Google, etc ont.

Il ne faut pas non plus oublier que certaines autorités peuvent être corrompues ou simplementagir dans leur propre intérêt. Les gouvernements et autres fournisseurs d'identités ont souventtrop de pouvoir et une trop grande confiance est placée en eux. De telles situations ne sontévidement pas en accord avec les intérêts de l'utilisateur et lui redonner le contrôle est d'autantplus important.

Il reste cependant un point qui n'est pas parfaitement clair. Les DIDs semblent être présentés comme améliorant la confidentialité des utilisateurs. Comme dis précédemment, les DIDs permettraient de ne fournir que les informations nécessaires sans avoir à en donner trop (histoire de la carte d'identité). Néanmoins, qu'est-ce qui garantit que fournisseur de services ne va pas trop en demander ? Certes il ne va plus demander la carte d'identité, mais il peut toujours demander chaque éléments de la carte un par un sans en avoir réellement besoin. Actuellement, rien ne permet de s'assurer qu'aucun risque n'est présent de ce côté là.

Service Provider

Le principal argument pour faire utiliser les DIDs à un Service Provider est le déplacement des risques. En effet, tous les risques relatifs à la vérification de l'identité, des VCs etc sont déplacés vers l'utilisateur. Le Service Provider a juste à faire la vérification cryptographique pour être sûr de ce qu'il reçoit, la véracité des informations n'est pas de son ressort.

De plus, le Service Provider n'a pas besoin de conserver les informations une fois celles-ci utilisées. Il n'aura qu'à les redemander la prochaine fois. Cela résout énormément de problèmes de confidentialité, de stockages de données, etc vis-à-vis de réglementations telles que le RGPD, mais résout aussi les problèmes liés au stockage en lui-même : plus besoin de serveurs de bases de données immenses pour stocker toutes les informations de tous les utilisateurs, réduction du risque de vol d'informations sensibles en cas de cyberattaques, etc.

Cependant, le Service Provider a besoin de savoir quels VCs il va accepter, et provenant de quels Issuers. Avoir beaucoup d'Issuers est pratique pour l'utilisateur mais peut vite devenir très compliqué à gérer pour les Services Providers.

Ce problème ne se présente pas avec les autres solutions de gestion d'identités. Dans le modèle en silo chaque Service Provider est indépendant et gère lui mêmes les identités, dans le modèle fédéré chacun se rapporte à l'autorité de la fédération d'identité et n'a besoin de faire confiance à personne d'autre, et dans le cas du système user-centric les Service Providers ne font confiance qu'à une liste bien précise de tiers de confiance et n'ont pas besoin d'en ajouter de nouveaux régulièrement.

Claims Issuers

Le choix des Claims Issuers quant à intégrer l'écosystème semble évident. En effet, il n'aurait aucune raison de ne pas vouloir l'intégrer, et il serait en plus en mesure d'accroître leur pouvoir.

Comme énoncé précédemment, même si les utilisateurs fournissent eux-mêmes leurs

informations, celles-ci doivent être certifiées par une autorité responsable (une mairie par exemple). De ce fait, les Claims Issuers gardent un pouvoir très important. De plus, une autorité est toujours en mesure de retirer une certification si l'information concernée a été modifiée, n'est plus valide, etc.

D'un côté cela permet d'assurer la conformité des informations que fourni l'utilisateur et ainsi éviter tout problème avec les Service Providers, mais d'un autre côté cela montre bien que l'utilisateur n'est pas tout à fait maître de son identité. Cependant, peut-on réellement laisser l'utilisateur totalement libre ? Il semble évident que non. Dans une telle situation, les informations erronées deviendraient rapidement courantes et ce système n'aurait plus aucune valeur ni crédibilité.

Fournisseurs de technologies

Les fournisseurs de technologies sont, entre autres, ceux qui développent la blockchain, mais aussi toute les organisations qui vont travailler sur les solutions d'authentification, etc. A première vue, ces fournisseurs n'auraient aucune raison d'être contre le développement des DIDs. Une nouvelle technologie permet de l'ouverture de nouveaux marchés et des gains financiers sont envisageables.

Cependant, tous ne voient pas ceci de la même manière. En effet, le développement complet d'une telle technologie nécessite des investissements financiers et humains colossaux, alors que des technologies similaires existent déjà. La blockchain peut-être faite avec les PKI, les Verifiable Credentials ne sont au final qu'une refonte des JSON Web Token, etc. De plus, l'aspect sécurité entre en jeu : les solutions déjà existantes ont été éprouvées et de nombreuses vulnérabilités ont déjà été patchées. Le développement des DIDs impliquent de tout reprendre à zéro sur ce point.

La question est donc : les coûts de développement engagés sont-ils justifiés par rapport à ce que va rapporter cette nouvelle technologie ? Là où les autres acteurs avaient une vision du problème centrée sur la praticité, la législation, la conformité, etc, les fournisseurs de services ont une vision essentiellement financières. Et si ils estiment que ce développement n'est pas rentable et qu'il n'est pas intéressant d'investir dedans, les DIDs n'ont finalement que peu de chance de voir le jour.

Conclusion

Cette première étude nous a permis d'avoir un aperçu de ce que sont les Decentralized Identifiers et ce qu'ils promettent de réaliser. Il s'agit de redonner un maximum de contrôle à l'utilisateur sur les informations qu'il choisi de fournir tout en assurant la validité de ces dernières, et limiter les stockages intempestifs de données.

Cependant, nous avons constaté que certaines questions restent en suspend, comme par exemple savoir si les informations demandées sont réellement nécessaires. De plus, tous les acteurs ne

sont pas encore sûr de vouloir s’engager pleinement dans le projet ce qui rend incertain sont développement.

Sources

Papier officiel W3C : https://www.w3.org/TR/did-core/

Synthèse par le W3C Community Group : https://w3c-ccg.github.io/did-primer/

Understanding Decentralized IDs (DIDs) – *Medium* :

https://medium.com/@adam_14796/understanding-decentralized-ids-dids-839798b91809

Résumé sur l’historique de la gestion de l’identité numérique :

https://www.silicon.fr/avis-expert/lidentite-auto-souveraine-et-la-blockchain-une-reponse-au-rgpd?fbclid=IwAR2LOG_rxHjl39dybCNaz8rzo9j56C3Zy0qtRGK9diYO8Z236onBZveibsY

Les pour et les contre de la fédération d’identité – *LeMagIT* : https://www.lemagit.fr/conseil/Pourset-contres-de-la-federation-didentite

---

Revision #2
Created 24 September 2022 00:21:58 by mxrch
Updated 1 November 2023 15:49:20 by BlackWasp