[Commencez ici](#_m2gfg0jlyssa)

[Bienvenue](#_o426ect7wrgy)

[Introduction](#_y4hwdz82qgde)

[À quoi s'attendre](#_cusimqwulciz)

[Besoin d'aide?](#_tds0y2794e80)

[Instructions de navigation](#_jy335t64e9ut)

[Pré-évaluation](#_3mlgtr6g0qn5)

[Module 1: Fondements des justificatifs numériques](#_bd0cb4t4oxya)

[Introduction](#_qc96jwj2nfiu)

[Objectifs d'apprentissage](#_4d34og8)

[Identité numérique et justificatifs, Définitions](#_w472hxqudi3q)

[Définition de l'identité et des justificatifs](#_fhblx76z5tjq)

[Personnes, organisations et représentants](#_o6kjfhq7hvix)

[Rencontrez Johanna](#_rqabmpcqdyu7)

[Justificatifs, identifiants et authentifiants](#_gahl7f3b34it)

[Assertions, validation et vérification](#_83a8q0c5xra3)

[Rencontrez Martin](#_6rgrref0pgob)

[Vérifiez votre compréhension](#_dbnqobhdij2h)

[Création d'un justificatif numérique](#_9tg3x4s3b5zm)

[Cycle de vie des justificatifs numériques](#_q7qnr0b6nugn)

[Le processus de création d'un justificatif numérique](#_9wfu3om7sg63)

[Plus d'informations sur la création d'un justificatif numérique](#_v2iq2dgusb87)

[Rencontrez Susan](#_wito72on9ab9)

[Vérifiez votre compréhension](#_pjwktcricgux)

[Entrevues avec des experts](#_eblff8fz811j)

[Entrevue avec Patrick Drolet](#_dzuvg25f4phy)

[Conclusion](#_nu90hqu91gb5)

[Questionnaire du module 1](#_eop8aa9m5li)

[Module 2 : Concepts relatifs aux justificatifs numériques](#_hek3ixfuj7ks)

[Introduction](#_jnm0whxvob02)

[Facteurs d'authentification et authentification multifacteur](#_vy6phswq27s4)

[Rencontrer Natalie](#_71iezj1qpf7w)

[Concepts importants relatifs aux justificatifs numériques](#_uoychjs3k7en)

[Introduction](#_sod17gca10au)

[Justificatifs vérifiables](#_g21t061vflxu)

[Identifiants décentralisés](#_b5iu5092jouc)

[Registre distribué](#_lopbekqep593)

[Vérifiez votre compréhension](#_jur9gpi1bgw9)

[Portefeuilles numériques](#_zfuwhgkn2vsm)

[Identité auto-souveraine](#_39mvw3mf6v3)

[Divulgation sélective](#_7ws94r71c28b)

[Preuve à divulgation nulle de connaissance](#_906kstyq09r5)

[Vérifiez votre compréhension](#_umml10y1zu9w)

[Entrevues avec des experts](#_1k2n7htjfdfe)

[Entrevue avec Andre Boysen](#_l57if4rmai8s)

[Entrevue avec Mathieu Desrosiers](#_x1qma7nwzqsy)

[Conclusion](#_tgebwmxj5l7s)

[Questionnaire du module 2](#_pimd5cdknr4q)

[Module 3 : Risque, protection de la vie privée et obstacles à l'adoption](#_34etiss29a5r)

[Introduction](#_gznqo761ax5y)

[Risque et niveau d'assurance (NdA)](#_vm0iziba77my)

[Qu'est-ce que le risque et le NdA?](#_kg4j5kcgmsk)

[Cadres des NdA](#_g47o7iqkcs5r)

[Exemple d’atténuation des risques](#_b61iasnyfyj0)

[Rencontrer Mike](#_bg1b8knrgvs4)

[Protection de la vie privée](#_p45jgnjo7ghw)

[Concepts et législation sur la protection de la vie privée](#_kestsrw45fgk)

[Protection de la vie privée dès la conception (Privacy by Design)](#_6c75rq8sncw)

[Rencontrez Amanda](#_32o4pnee7ph7)

[Facteurs qui influencent l'adoption des justificatifs numériques](#_2wqpd82izec6)

[Les cinq facteurs clés](#_oy1cu92pib3a)

[Rencontrez John](#_4s7ozgnovm39)

[Vérifiez votre compréhension](#_3u2f8op0tmz3)

[Entrevues avec des experts](#_ng4g6gd07xc9)

[Entrevue avec Catherine Desgagnes-Belzil](#_9j6wfa3udr4g)

[Entrevue avec Dr. Ann Cavoukian](#_tr1wtqeq5qh1)

[Entrevue avec Michelle Chibba](#_m0n6vwvmoysi)

[Conclusion](#_kdc71if8wtim)

[Questionnaire du module 3](#_aojssivg8crd)

[Module 4 : Modèles d'écosystèmes et justificatifs vérifiables](#_o20sflwybbvy)

[Introduction](#_puabiqp9tq74)

[Écosystèmes d'identité numérique](#_fqqov2ttz2hv)

[Définir l'écosystème de l'identité numérique](#_580wg672069c)

[Considérations importantes](#_f7vl8oud04q1)

[Confiance](#_86icyibgkefa)

[Standards et cadres de référence](#_ydej2vf1cysi)

[Qu'est-ce que le Cadre de confiance pancanadien (CCP)?](#_bxvvxtj4vk2y)

[Processus standardisés du CCP](#_mpkaaigphhyb)

[Autres travaux notables au Canada et dans le monde](#_3hjngbsvxan5)

[Plus de travaux internationaux](#_fpoaygxxkwhf)

[Vérifiez votre compréhension](#_spbhr6sokn33)

[Modèles d'écosystèmes](#_8s9z6up53q3m)

[Définir les modèles](#_316vs9u26yr2)

[Centralisé](#_ciqjqr1ipvy5)

[Fédéré](#_4codfrhbhfnn)

[Décentralisé](#_wqb6fy1nqj7y)

[Caractéristiques des écosystèmes sains](#_9kn4rbw6rp06)

[Retour sur Martin](#_upoi69dnoyha)

[Entrevues avec des experts](#_uk1b9dc0bij2)

[Entrevue avec Joni Brennan](#_k6b56rvd6xr0)

[Entrevue avec Andrew Johnston](#_cn917ai4e12u)

[Conclusion](#_o55lo8acibrd)

[Questionnaire du module 4](#_65q0in74xnf0)

[Module 5: Justificatifs vérifiables](#_hfu1mrcu95ag)

[Introduction](#_dfi8wsf8uezi)

[Justificatifs vérifiables et identité vérifiée](#_fi1m33u8arr)

[Justificatifs vérifiables](#_ra92gk4pjsz8)

[Comment fonctionnent les justificatifs vérifiables?](#_dzqffszd27wd)

[Comment fonctionnent les assertions vérifiables?](#_4rcbhinrodvh)

[Délivrance et utilisation d'un justificatif d'identité](#_dtqq811sigju)

[Constitution d'un justificatif vérifiable](#_mo24pl1ophdy)

[Délivrance de justificatifs vérifiables](#_2rjmy2owuh0t)

[Assertions vérifiables](#_rqmf86abo23k)

[Justificatifs vérifiables et assertions vérifiables en action](#_wwdbnei802mc)

[Identifiants décentralisés](#_3pff8o18h796)

[Vérifiez votre compréhension](#_vxk9yiolgbx3)

[Entrevue avec des experts](#_z5ke2jftxg1k)

[Conclusion](#_8t65t9vwt22r)

[Questionnaire du module 5](#_dryrcz6njud1)

[Module 6: Considérations liées à la conception des solutions d'identité numérique](#_yms403dexybp)

[Introduction](#_4ip0vnwsvrna)

[Objectifs d'apprentissage](#_49x2ik5)

[La cryptographie](#_oxw12480xrt4)

[Introduction à la cryptographie](#_8e5z8po7hrfl)

[Le chiffrement asymétrique en action](#_fmhyjram53o9)

[Approches de chiffrement](#_te1t0q9vav0z)

[Signatures numériques](#_34tg07aidw0j)

[La divulgation sélective](#_gxiwzdf48jny)

[Introduction à la divulgation sélective](#_ahbparp5gttf)

[Exemple de divulgation sélective](#_ghz1alxfcz92)

[Divulgation nulle de connaissance](#_ekii16i6mqx3)

[Introduction à la preuve à divulgation nulle de connaissance](#_ikejt24fpn3h)

[Critères de la preuve à divulgation nulle de connaissance](#_tjlpjft1pso0)

[Portefeuilles numériques](#_8daekjk28uyc)

[Portefeuilles numériques](#_33eity4h5p5w)

[Qu'est-ce qu'un portefeuille numérique et comment fonctionne-t-il?](#_z3mhoul57htu)

[Exemple de portefeuille numérique](#_xnvscybd9k6x)

[Vérifiez votre compréhension](#_c1j5lw373q91)

[Identité auto-souveraine](#_3ksf17epbcxs)

[Introduction à l'identité auto-souveraine](#_n9ynmr6c72zk)

[Gouvernance](#_fyusl83tisqw)

[Définition des rôles clés](#_3w2sa9yvjkqn)

[Un justificatif vérifiable](#_5ls7iiougk6a)

[Identifiants distribués](#_ja1d5gnp2vv7)

[Portefeuilles numériques](#_nxxqo9mu69w)

[Agents logiciels](#_kuv6yjtpbkzp)

[Registre distribué](#_tlwk7kg4ckzc)

[Chaîne de blocs](#_kws2sadvtwpj)

[Trust over IP](#_53d14lb0a3ua)

[Introduction à Trust over IP](#_ws6ynmalcra)

[La pile Trust over IP (Trust over IP Stack)](#_rcr5ym717qvf)

[Vérifiez votre compréhension](#_b73j36519lkq)

[Entrevues avec des experts](#_nl3ggre18d06)

[Entrevue avec Tim Bouma](#_ulvzw8cmbzvo)

[Entrevue avec Peter Watkins](#_r2txmqtnhik0)

[Entrevue avec Ian Bailey](#_7gd5kfjb3nds)

[Conclusion](#_grmi1i7wsv9w)

[Questionnaire du module 6](#_h9mp2ue1r5fn)

[Module 7 - Technologies et cadres de référence](#_8p3zy3xlp1q0)

[Introduction](#_anzzwds9hapw)

[Objectifs d'apprentissage](#_vkudlbukotz5)

[Standards ouverts](#_5f6bdakhl57)

[Identité fédérée, les standards technologiques couramment utilisés](#_s6z6u9c4i334)

[SAML - Security Assertion Markup Language](#_dg14c9m0zqbu)

[OpenID Connect](#_pcv91pmoyywc)

[OAuth](#_29aaww9xenh1)

[Jetons Web](#_voic8m8oj1mr)

[Vérifiez votre compréhension](#_oi8nfzxodecj)

[Modèles de justificatifs numériques pair à pair, les standards technologiques couramment utilisés](#_v18yd61sfqei)

[Nous examinerons plusieurs standards technologiques ou cadres de référence différents qui ont été utilisés dans les mises en œuvre de référence de justificatifs vérifiables. Nous nous pencherons principalement sur la manière dont les justificatifs vérifiables sont exprimés, et sur la manière dont ils sont signés et prouvés numériquement.](#_pwsn37z40pxg)

[JSON and JSON-LD](#_g8ofojve51tv)

[Conteneurs de justificatifs vérifiables](#_dumgq9dzud4t)

[Chaîne de blocs](#_4kg0yjot5nt6)

[Implantation de la chaîne de blocs avec permission](#_d9dds8wjo072)

[Plus d'informations sur la chaîne de blocs](#_z06x70av80pt)

[Hyperledger](#_kg889w3xuwqf)

[Divulgation sélective](#_4u3z0cnl3h6q)

[Introduction à la technologie relative à la divulgation sélective](#_3kd4d0ib22k9)

[Signatures numériques multimessages](#_nl835ht3vlwx)

[Exemple de divulgation sélective](#_q0vcatbsva0p)

[Vérifiez votre compréhension](#_39h458gmy4qc)

[Entrevue avec des experts](#_wv2zilfgqpoi)

[Entrevue avec Kaliya Young (Identity Woman)](#_5o9kr2wn7yig)

[Entrevue avec John Jordan](#_7louu8sryhmq)

[Conclusion](#_fxhlczdham2p)

[Questionnaire du module 7](#_aodaaz58ugxc)

[Post-évaluation](#_mnvulmcegb87)

Introduction aux justificatifs numériques

# 

# Commencez ici

## Bienvenue

### Introduction

Bienvenue à la formation « Introduction aux justificatifs numériques »!

Ce portail d'apprentissage gratuit, accessible à votre rythme et disponible sur demande, a été créé pour introduire et renforcer les connaissances des utilisateurs en matière de justificatifs numériques, y compris la manière de déployer des justificatifs numériques qui améliorent la protection de la vie privée, qui sont conformes à la loi et qui sont interopérables de manière durable.

Nous anticipons et accueillons des utilisateurs des secteurs privé et public ayant des niveaux d'expérience différents. Ultimement, l'objectif de ce portail d'apprentissage est de fournir au public intéressé une vue complète des justificatifs d’identité numériques pour prendre des décisions d'investissement éclairées ou exécuter des plans de projet de transformation numérique réussis.

L’objectif de la formation est d’acquérir des connaissances de base.

**Objectifs de la formation**

À la fin de la formation, les participants seront en mesure de :

* Définir les termes et les concepts couramment utilisés lorsqu’il est question de justificatifs numériques.
* Expliquer les principaux enjeux juridiques, opérationnels, technologiques et en matière de protection de la vie privée, de même que les opportunités liées aux justificatifs numériques.
* Décrire les tendances actuelles en matière de conformité et d'interopérabilité en lien avec les justificatifs numériques.
* Décrire les cas d'utilisation essentiels liés à la gestion des justificatifs vérifiables.
* Présenter un cadre d'analyse parfaitement adapté pour fournir des solutions conformes et interopérables aux cas d'utilisation des justificatifs numériques.

### À quoi s'attendre

**Détails sur la formation**

Commençons par expliquer comment la formation est conçue et ce à quoi vous devez vous attendre.

La formation est divisée en sept modules. Chacun de ces modules présentera de nouveaux sujets et concepts. En voici la répartition :

| **Module** | **Titre** |
| --- | --- |
| 1 | Fondements des justificatifs numériques |
| 2 | Concepts relatifs aux justificatifs numériques |
| 3 | Risque, protection de la vie privée et obstacles à l'adoption |
| 4 | Modèles d'écosystèmes et justificatifs vérifiables |
| 5 | Justificatifs vérifiables |
| 6 | Considérations liées à la conception des solutions d'identité numérique |
| 7 | Technologies et cadres de référence |

**À quoi s'attendre**

Vous devrez commencer par le module 1, lequel couvre les principes de base. Lorsque vous aurez terminé ce premier module, vous pourrez progresser dans le reste de la formation dans l'ordre de votre choix.

La formation commencera par une pré-évaluation. Cette évaluation préalable est destinée à tester les connaissances que vous avez déjà. Ne vous souciez pas de répondre correctement aux questions, répondez simplement au meilleur de vos connaissances.

Chaque module comprend diverses ressources d'apprentissage, comme des liens vers des sites internet, des graphiques, des vidéos explicatives, des entrevues, etc. Vous aurez également des occasions de vous arrêter et de vous évaluer. Cela permet de s’assurer que vous avez bien saisi les principaux concepts avant de poursuivre. Vous pouvez effectuer ces courtes auto-évaluations autant de fois que vous le souhaitez. À la fin de chaque module, un questionnaire noté permet d'évaluer votre compréhension des concepts abordés. Vous pouvez prendre le temps que vous voulez pour répondre à ces questionnaires, et nous vous encourageons à le faire. N'oubliez pas que vous n'avez qu'une seule tentative.

À la fin de la formation, vous effectuerez une évaluation finale, comme la pré-évaluation que vous avez effectuée au début de la formation, afin de déterminer si vous avez atteint les objectifs d'apprentissage et les buts de la formation. L'évaluation finale peut être également effectuée dans un temps illimité.

### Besoin d'aide?

Pour toute assistance concernant la formation, veuillez envoyer un courriel à: [education@idlab.org](mailto:education@idlab.org).

### Instructions de navigation

Vous avez probablement remarqué que vous ne pouvez voir que la page « Commencez ici » et le module 1. C'est intentionnel. Nous voulons que vous commenciez par les bases avant de poursuivre. C'est utile pour les personnes qui découvrent ce sujet et pour celles qui ont de nombreuses années d'expérience. Il existe différentes façons de décrire ou de définir plusieurs des termes que nous utilisons fréquemment dans la formation. Il est important d'avoir une compréhension générale de ces termes dès le début.

Une fois que vous avez terminé le module 1, les 6 autres modules sont disponibles. Il vous suffit de sélectionner le titre du module pour faire apparaître les thèmes qui le composent. Sélectionnez le premier thème sous le module choisi et parcourez le contenu à l'aide des flèches «Suivant» et «Précédent» situées en haut et en bas de la page.

Encore une fois, cette formation se déroule à votre rythme et vous pouvez l'interrompre et la reprendre à tout moment. Le système est configuré pour suivre les pages que vous avez visitées et indique un crochet vert à côté de la page précédemment consultée. Cela vous aidera à reprendre la formation là où vous l'avez laissée.

NOTE IMPORTANTE: Pour que les autres modules apparaissent, vous devez examiner chaque page de chaque sous-thème du module 1 et répondre à tous les questionnaires. La coche verte vous indique que vous avez consulté une page. S'il n'y a pas de coche verte, revenez en arrière et relisez cette page.

Lorsque vous arrivez à la fin d'un module, vous ne pourrez plus cliquer sur le bouton «Suivant», ce qui indique que vous êtes sur la dernière page. Dans ce cas, il vous suffit de sélectionner «Formation» dans le menu de navigation et de là, vous pourrez accéder au module suivant que vous souhaitez consulter.

En cas de problème, n'hésitez pas à envoyer un courriel à : [education@idlab.org](mailto:education@idlab.org).

## Pré-évaluation

Bienvenue au projet pilote sur les approches éducatives.

Nous sommes heureux de vous compter parmi les participants à cette initiative intéressante!

Pour commencer, nous aimerions vous poser quelques questions. Les informations recueillies seront utilisées pour concevoir et évaluer le programme éducatif. Il y a 28 questions au total, nous estimons qu’il faudra environ 10 à 15 minutes pour y répondre.

Conditions d'utilisation

Merci et nous sommes impatients de partager notre programme avec vous!

*L'équipe d'Innovation, science et développement économique (ISDE)*

*Digital Identity Lab / Laboratoire d'identité numérique*

>>1. Un mot de passe est un exemple de/d’\_\_\_\_\_\_\_\_\_\_\_\_\_. <<

( ) justificatif

( ) vérificateur

(x) authentifiant

( ) attribut d'identité

>>2. \_\_\_\_\_\_\_\_\_ confirme l'exactitude des informations présentées, tandis que \_\_\_\_\_\_\_\_\_ assure qu'elles appartiennent à l'entité à laquelle s'applique l'assertion d'identité. <<

(x) La validation, la vérification

( ) L’authentification, la validation

( ) L’authentification, la vérification

( ) La vérification, la validation

>>3. Une preuve \_\_\_\_\_\_\_\_\_\_\_ en matière de justificatifs ne s'applique qu'à une personne ou une organisation légalement reconnaissable. <<

( ) numérique

(x) fondamentale

( ) contextuelle

( ) authentique

>>4. Votre justificatif peut être utilisé pour accéder à quelque chose (par exemple, un service en ligne) <<

( ) Vrai

(x) Faux

>>5. \_\_\_\_\_\_\_\_\_\_\_\_ est le processus qui consiste à établir que le sujet du justificatif numérique peut être décrit de manière à être unique dans l'ensemble des justificatifs numériques délivrés. <<

( ) La validation

( ) La vérification

( ) L’authentification

(x) La résolution

>>6. Le gouvernement fédéral a formellement défini \_\_ niveaux d'assurance (NdA) pour les justificatifs numériques. <<

( ) 2

(x) 4

( ) 6

( ) 8

>>7. La/Les \_\_\_\_\_\_\_\_\_ définit/définissent la façon dont le gouvernement fédéral doit traiter les renseignements personnels. <<

(x) *Loi sur la protection des renseignements personnels*

( ) LPRPDE

( ) PIPA

( ) lois provinciales sur la protection des renseignements personnels

>>8. Les \_\_\_\_\_\_\_\_\_\_\_\_ expriment les objectifs et les intentions d'une organisation, tandis que les \_\_\_\_\_\_\_\_\_\_\_\_ définissent formellement ce qui sera fait et comment. <<

( ) règlements, standards

( ) standards, politiques

( ) procédures, règlements

(x) politiques, procédures

>>9. « Les menaces à la vie privée devraient être anticipées et prévenues avant qu'elles ne se produisent » fait partie \_\_\_\_\_\_\_\_\_\_. <<

( ) de la LPRPDE

( ) des 10 principes relatifs à l'équité dans le traitement de l'information

(x) de la protection de la vie privée dès la conception

( ) de la *Loi sur la protection des renseignements personnels*

>>10. La capacité de démontrer que les processus de traitement des renseignements personnels sont conformes au niveau d'assurance (NdA) attendu est un élément à prendre en considération lors de l'évaluation de la/de l’\_\_\_\_\_\_\_\_\_\_. <<

( ) protection de la vie privée

( ) convivialité

( ) interopérabilité

(x) responsabilité

>>11. La clé d'un écosystème de justificatifs numériques viable est la/le \_\_\_\_\_\_\_\_\_\_. <<

( ) fiabilité

( ) respect des standards

(x) confiance

( ) convivialité

>>12. La/Le \_\_\_\_\_\_\_\_\_ crée un cadre pour la confiance et l'interopérabilité des justificatifs numériques au Canada. <<

( ) Directive sur la gestion de l'identité

( ) Conseil canadien des normes

(x) Cadre de confiance pancanadien (CCP)

( ) W3C

>>13. Les deux standards souvent cités lors de l'étude des justificatifs vérifiables et de l'identité décentralisée sont le standard *data model for verifiable credentials* et le standard *specification for decentralized identifiers* publiés par le/l’ \_\_\_\_\_\_\_. <<

( ) ISO

(x) W3C

( ) NIST

( ) IETF

( ) CCIAN

>>14. Les modèles d'identité fédérée permettent aux utilisateurs de mieux contrôler leurs renseignements personnels. <<

( ) Vrai

(x) Faux

>>15. Les fournisseurs d'identité de confiance sont la clé des justificatifs vérifiables tels que décrits dans les standards du W3C. <<

( ) Vrai

(x) Faux

>>16. La preuve de la délivrance d'un justificatif sans en révéler le contenu réel est appelée \_\_\_\_\_\_\_\_\_\_\_. <<

( ) la divulgation sélective

(x) la preuve à divulgation nulle de connaissance

( ) un justificatif vérifiable

( ) l’identité auto-souveraine

>>17. Le « triangle de la confiance », souvent utilisé pour décrire les justificatifs numériques, comprend \_\_\_\_\_\_\_\_, le titulaire et le vérificateur. <<

(x) l’émetteur

( ) le sujet

( ) le fournisseur d'identité

( ) le fournisseur de services

>>18. Les standards *Linked Data* (données liées) étendent les standards technologiques existants afin de fournir \_\_\_\_\_\_\_\_\_\_ pour les données échangées. <<

( ) une meilleure sécurité

( ) une interopérabilité renforcée

(x) du contexte

( ) d’autres méthodes

>>19. Le vérificateur d'un justificatif vérifiable doit consulter l'émetteur d'un justificatif pour s'assurer que le justificatif est valide. <<

( ) Vrai

(x) Faux

>>20. Les informations des justificatifs ne sont jamais stockées dans le registre distribué dans le modèle de l’IAS. <<

(x) Vrai

( ) Faux

>>21. Les justificatifs vérifiables sont faciles à manipuler, et il faut s'en prémunir. <<

( ) Vrai

(x) Faux

>>22. Avec les justificatifs vérifiables, un changement d'information nécessite la révocation et la délivrance d'un nouveau justificatif. <<

(x) Vrai

( ) Faux

>>23. Dans les modèles de justificatifs numériques pair à pair ou décentralisés, le titulaire d'un justificatif numérique est toujours le sujet du justificatif numérique. <<

( ) Vrai

(x) Faux

>>24a. Sur une échelle de 1 à 5, en considérant ce que vous savez maintenant, comment évaluez-vous la capacité de votre organisation pour la mise en œuvre d'un système dépendant des justificatifs numériques? Évaluez et tapez votre réponse dans l'espace prévu à cet effet. <<

( ) 1 (faible)

( ) 2

( ) 3

( ) 4

( ) 5 (très élevée)

( ) S. O. - Je ne suis pas sûr(e)

>>24b. Quelles sont les lacunes que vous percevez / de quoi votre organisation aurait-elle besoin pour atteindre ces objectifs? <<

= réponse

>>25a. Sur une échelle de 1 à 5, en considérant ce que vous savez maintenant, comment évaluez-vous la capacité de votre organisation pour la mise en œuvre d'un système dépendant des justificatifs numériques et basé sur des technologies émergentes telles que les portefeuilles numériques et la chaîne de blocs (*blockchain*)? <<

( ) 1 (faible)

( ) 2

( ) 3

( ) 4

( ) 5 (très élevée)

( ) S. O. - Je ne suis pas sûr(e)

>>25b. Quelles sont les lacunes que vous percevez / de quoi votre organisation aurait-elle besoin pour atteindre ces objectifs? <<

= réponse

>>26. Sur une échelle de 1 à 5, quel est votre degré de confiance dans votre connaissance des lois, règlements et politiques applicables aux justificatifs numériques? <<

( ) 1 (faible)

( ) 2

( ) 3

( ) 4

( ) 5 (très élevé)

( ) S. O. - Je ne suis pas sûr(e)

>>27a. Sur une échelle de 1 à 5, comment évaluez-vous votre niveau de confiance dans les justificatifs numériques? <<

( ) 1 (faible)

( ) 2

( ) 3

( ) 4

( ) 5 (très élevé)

( ) S. O. - Je ne suis pas sûr(e)

>>27b. Quelles sont les lacunes que vous percevez / quelles sont vos préoccupations concernant les justificatifs numériques? <<

= réponse

>>28a. Sur une échelle de 1 à 5, comment évalueriez-vous votre intérêt ou celui de votre organisation à adopter des justificatifs numériques? <<

( ) 1 (faible)

( ) 2

( ) 3

( ) 4

( ) 5 (très élevé)

( ) S. O. - Je ne suis pas sûr(e)

>>28b. Quelles sont les lacunes que vous percevez / de quoi auriez-vous besoin, vous ou votre organisation, pour atteindre ces objectifs? <<

= réponse

# Module 1: Fondements des justificatifs numériques

## Introduction

Bienvenue dans le module sur les fondements des justificatifs numériques! Alors, vous souhaitez en savoir plus sur les justificatifs numériques. Pour ce faire, vous devez d'abord comprendre les concepts fondamentaux et le lexique de base. Ce module vous présente ces termes et ces concepts.

Par exemple, qu'est-ce que l'identité? Qu’est-ce que les identités numériques et les justificatifs? Qu’est-ce que les justificatifs vérifiables? Si vous avez du mal à trouver une définition claire dans votre esprit, ne vous inquiétez pas! Ce module couvre les bases de manière claire et concise. Ceci est essentiel pour que vous ayez une bonne compréhension de la terminologie qui vous permettra de saisir les concepts qui seront abordés dans les modules suivants.

Il est important de définir les concepts relatifs aux justificatifs numériques de manière simple, car sans une base sémantique commune sur ceux-ci, il est plus difficile de stimuler la croissance économique et l'innovation qui peuvent être réalisées grâce à des justificatifs numériques.

## Objectifs d'apprentissage

* Définir les justificatifs, les identifiants, les entités et les attributs.
* Reconnaître l'interconnexion entre l'assertion, la validation et la vérification.
* Examinez les concepts de justificatifs d'identité et d'authentifiants.
* Explorer le cycle de vie d'un justificatif numérique.

## Identité numérique et justificatifs, Définitions

### Définition de l'identité et des justificatifs

Commençons par les bases. Prenez un moment pour réfléchir à comment vous concevez l’identité. Si quelqu'un est assis à côté de vous en ce moment, demandez-lui comment il définirait l'identité. Avez-vous des définitions similaires?

Dans la société, vous avez une identité en tant qu'individu, une personne indépendante du papier, du plastique ou de toute autre forme de représentation. Votre identité est une *assertion de qui vous êtes*. C'est qui vous êtes, comment vous agissez dans le monde, comment vous interagissez avec lui. Dans cette interaction avec le monde, cependant, nous avons besoin de la capacité de prouver des faits.

Ces preuves se répartissent en deux catégories. L'**identification**, qui prouve que vous êtes bien la personne que vous prétendez être, et les **justificatifs** qui prouvent tout, allant de l'éducation à l'autorisation de conduire un véhicule à moteur.

Une société numérique exigera en grande partie ce dont nous avons besoin aujourd'hui dans le monde physique. Votre identité est une identité numérique, et une série de justificatifs numériques vous permettent de faire face à la vie quotidienne. Les justificatifs numériques sont des représentations électroniques des assertions d'une identité ou des attributs de cette identité. Les justificatifs numériques sont ce que vous présentez pour faire une assertion d'identité, allant de « Je suis John Doe » à « Je suis John Doe, conducteur titulaire d'un permis de conduire du Manitoba ».

Compte tenu de l'incidence de phénomènes tels que l'usurpation d'identité et les fuites de données, certains pourraient se demander pourquoi ils voudraient une identité numérique en premier lieu. La réponse intuitive et évidente est la commodité que nous offre l'identité numérique. Le justificatif d'identité que vous transportez dans votre portefeuille est limité quant au nombre de transactions que vous pouvez réaliser avec celui-ci. Votre justificatif numérique peut théoriquement être utilisé avec toute personne avec qui vous souhaitez effectuer une transaction, à condition qu'elle soit présente en ligne. À la fin de ce programme d'apprentissage, vous constaterez également que les technologies et les standards émergents peuvent permettre de créer un justificatif numérique plus sécurisé et protégeant davantage la vie privée que le justificatif physique que vous transportez sur vous.

Nous devons également nous demander qui, ou quoi, peut avoir une identité. Si nous comprenons tous intuitivement qu'une personne physique a une identité, l'identité peut s'appliquer à d'autres choses, comme à une organisation (par exemple, une entreprise ou une association plus informelle) ou à une chose (par exemple, votre réfrigérateur dans un réseau d'appareils domestiques). Nous appellerons tout ce qui peut être identifié, dans un contexte spécifique, une « **entité »**.

Maintenant que vous avez une compréhension de base de ce que sont l'identité et les justificatifs, étudions des concepts supplémentaires et approfondissons un peu plus les concepts.

### Personnes, organisations et représentants

L'identité est le point de départ de toute relation. Elle est au cœur de l'authenticité des interactions sociales. Le plus souvent, elle permet d’instaurer la confiance et de l’assurance dans les interactions en cours entre les individus, ainsi qu’entre le gouvernement et les entreprises et les personnes ou organisations qu'il sert. L'identité dépend également du contexte. Le contexte peut être utilisé pour établir des éléments tels que des autorisations, un statut, des droits, ou pour transmettre des caractéristiques telles qu'une compétence particulière ou un résultat. Dans un contexte d'identité ou de justificatifs numériques, il est essentiel de pouvoir distinguer les entités les unes des autres pour que les services puissent être fournis au bon destinataire (pensez à l'identité numérique de confiance) et maintenir l'intégrité des processus d’affaires.

Nous avons parlé d'une entité comme étant toute personne ou toute chose qui peut être identifiée. Il convient de noter deux autres termes spécifiques, ainsi que leur signification. Tout au long de ce programme d'apprentissage, nous ferons référence à certains types précis d'entités, à savoir les **personnes** et les **organisations**.

| Personne | Organisation |
| --- | --- |
| Pour nos besoins, nous définirons une « **personne** » comme étant un être humain, vivant ou décédé. | Une **organisation** est souvent définie comme une entité légalement constituée, telle qu'une entreprise enregistrée ou un organisme de bienfaisance enregistré (ou immatriculé(e), pour le Québec). Les entités gouvernementales officielles sont également incluses dans la plupart des définitions de l'organisation. Cependant, dans certains cas, l'organisation a été définie de manière un peu plus large pour inclure des entités constituées de manière informelle. Dans le domaine de l'identité, cela est rare, mais pour les besoins de ce programme d'apprentissage, vous pouvez considérer que la notion d’**organisation** peut inclure des entités moins formellement constituées, selon la nature du programme ou du service nécessitant une identité numérique sécurisée. |

Plus tôt, nous avons parlé du contexte. Il est important de noter qu'une seule entité identifiable, par exemple une personne, peut avoir de nombreux contextes différents et des justificatifs numériques associés. John Doe peut être «John Doe le contribuable» et «John Doe, ingénieur mécanique chez ACME inc.» et «MEGASTRIKER, le fanatique des jeux en ligne». Chacun de ces contextes est susceptible d'avoir son propre justificatif numérique distinct et délivré pour être utilisé dans chacun de ces contextes.

Il existe différents types d'identité et de preuves d'identité. Les preuves d’identité **fondamentale** reposent sur des événements fondamentaux basés sur des faits qui peuvent être utilisés pour établir une identité fondamentale, ou plus précisément, l'existence d'une personne ou d'une organisation légalement reconnaissable. Les meilleurs exemples sont la naissance ou l'immigration pour les personnes, et la constitution en société pour une entité commerciale enregistrée. Au Canada, l'identité fondamentale relève exclusivement du secteur public (*c.-à-d*. les registres provinciaux des naissances, les registres des entreprises, etc.). L'identité **contextuelle** est une identité utilisée dans un but précis, dans un contexte précis. Les preuves d'identité créées au cours du processus d'établissement de ce type d'identité peuvent être considérées comme des preuves **contextuelles**. Parmi les exemples d'identité contextuelle et des preuves associées, on peut citer les justificatifs d’identité bancaires, les permis de conduire, ou même quelque chose d'aussi simple qu'un compte valide sur les médias sociaux.

Il existe une autre entité qui joue un rôle dans certains des processus liés à l'utilisation des justificatifs numériques. Il arrive souvent qu'une personne ou une organisation désigne quelqu'un pour agir en son nom. C'est particulièrement vrai dans le cas d'une organisation où une personne doit exécuter une transaction au nom d'une entreprise. Ce sont des **représentants**.

### Rencontrez Johanna

Examinons un exemple de création et d'utilisation d’un justificatif numérique d’affaires. Nous verrons comment un représentant est utilisé et certaines des questions propres à l'utilisation de justificatifs d'affaires.

<<Johanna video goes here>>

### Justificatifs, identifiants et authentifiants

Il y a quelques autres termes importants utilisés dans ce programme d'apprentissage que nous devons définir. Ils vous aideront à mieux comprendre les justificatifs numériques et la composition d'un justificatif numérique.

**Définition des justificatifs et des authentifiants**

La création d'une identité numérique va souvent de pair avec la création d'un **justificatif d'identité** et d'un **authentifiant** qui facilitent l'utilisation de cette identité numérique par une personne, ou une personne agissant au nom d'une organisation.

Un **justificatif numérique** est une représentation numérique de l'ensemble des informations d'identité et des autres informations qui peuvent être associées de manière unique au **sujet** (par exemple, une personne ou une organisation) d'une identité. Un **authentifiant** est un élément sous le contrôle du **sujet** d'un justificatif numérique qui lui permet d’affirmer que l'identité numérique est la sienne.

**Justificatifs vs authentifiants**

Prenons un exemple pour expliquer en quoi ces éléments peuvent être différents.

Lorsque vous cherchez à accéder à des services bancaires en ligne, la banque vous demande de vous présenter à une de ses succursales et de fournir des preuves de votre identité. Ces preuves permettent à la banque d'exercer sa propre vérification diligente pour décider de créer ou non un justificatif numérique. À l'issue de ce processus, la banque enregistre les informations qu'elle juge importantes à associer à une identité numérique et crée un **identifiant** qui lui permet de faire référence à l'identité numérique de manière unique. Cet identifiant peut être quelque chose d'aussi simple qu'un numéro de client unique qu'elle génère.

La somme totale de ces informations enregistrées peut être considérée comme le **justificatif d'identité**. Une fois l'identité numérique créée, la banque vous demande de créer un NIP ou un mot de passe pour vous permettre d'accéder aux services bancaires en ligne. Elle peut également vous demander de choisir quelques questions et réponses pour vous aider à accéder aux services bancaires en ligne. Le mot de passe et les réponses aux questions peuvent être considérés comme des **authentifiants**.

**Que contient un justificatif numérique?**

Un **identifiant** est un indicateur qui pointe vers une entité déterminée. Un identifiant peut être unique dans un système défini, comme le numéro d'assurance sociale (NAS) au Canada. Les numéros de permis de conduire et les numéros d'employés sont d'autres exemples d'identifiants. Pour les organisations, des exemples similaires pourraient être les numéros d'enregistrement des sociétés (uniques) ou les classifications des industries (non uniques).

Un **attribut** est une propriété ou une caractéristique susceptible d'être partagée par de nombreuses entités. Les attributs peuvent être professionnels (par exemple: avocat, ingénieur, architecte). Les attributs peuvent également être des affiliations (par exemple: employé d'une entreprise, membre d'une association d'anciens étudiants), des caractéristiques physiques (par exemple: couleur des yeux, sexe, taille), etc. Enfin, les attributs peuvent également être en rapport avec des personnes morales, comme la taille d'une entreprise (par exemple, petite et moyenne).

**Lier** un identifiant ou un attribut à une entité implique généralement que l’entité doit avoir un moyen de prétendre légitimement à l'identifiant ou à l'attribut. Lier est l'action d'enregistrer de manière fiable la relation entre un ensemble d'identifiants ou d'attributs et la personne ou l'organisation. Un justificatif numérique peut contenir des attributs qui sont créés dans le seul but de soutenir le lien.

### Assertions, validation et vérification

**Assertion**

Avec le lien entre les identifiants et les attributs d'une entité (c'est-à-dire les personnes, les organisations et les entités), et la délivrance d'un justificatif numérique, un justificatif numérique peut être utilisé pour faire une assertion concernant l'identité. Il peut s'agir, par exemple, d’accéder à un service (comme une entreprise qui interagit avec un programme gouvernemental ou une personne qui effectue une transaction bancaire, en personne ou en ligne) ou de l'établissement de l'identité dans un certain nombre de contextes d'interaction sociale.

Il y a quelques concepts supplémentaires qui doivent être définis. Chaque fois qu'une identité est prétendue par quelqu'un ou quelque chose, il y a une **assertion** de l'existence de cette identité et des preuves qui la soutiennent. Il peut s'agir d'une **autodéclaration** ou d'une assertion corroborée par un tiers de confiance.

**Validation et vérification**

Plus tard, lorsque nous examinerons les processus de création et d'utilisation d'un justificatif numérique, nous rencontrerons deux autres concepts importants. Il s'agit de la **validation** et de la **vérification**. Examinons-les en utilisant l'exemple suivant pour fournir un contexte.

Vous faites l'objet d'un contrôle routier par la police en vous rendant à votre domicile et le policier vous demande d'abord qui vous êtes et où vous habitez. Vous indiquez votre nom et fournissez votre permis de conduire comme preuve. À ce stade, vous avez fait une **autodéclaration** de votre identité et fourni des justificatifs. L'agent retourne ensuite à sa voiture avec votre permis et consulte le registre provincial des conducteurs pour s'assurer que vous êtes bien la personne que vous prétendez être et que l'assertion est exacte. Cette deuxième vérification indique au policier que le numéro du permis de conduire existe et qu'un tiers de confiance (c'est-à-dire le bureau des permis de conduire) a suivi son propre processus de vérification de l’existence de votre identité.

Le policier a suivi d’autres processus importants au cours de cette interaction.

1. Il y a eu une **validation** des attributs et des identifiants utilisés pour soutenir l'assertion d'identité que votre justificatif représente. La **validation** est le processus qui consiste à *confirmer l'exactitude des informations présentées*. Dans ce cas, le nom que vous avez déclaré a été vérifié à l’aide du permis. L'âge approximatif et d'autres attributs disponibles sur le permis ont également été vérifiés pour confirmer l'exactitude des informations présentées.
2. La **vérification** est le processus qui consiste à *confirmer que l'identité prétendue appartient de manière unique à l'entité qui la prétend* (dans ce cas, vous). Le policier a effectué une première vérification en comparant la photo figurant sur votre permis à vous-même, estimant que le visage d'une personne est relativement unique. Une vérification secondaire a été effectuée lorsque le policier a consulté le bureau provincial des permis de conduire pour s'assurer que les preuves présentées étaient valides. Par la même occasion, il a su qu'un tiers de confiance avait également effectué son propre processus de validation et de vérification avant de délivrer le permis de conduire.

Ces efforts de validation et de vérification ont permis au policier d'accepter l'assertion d'identité, telle que représentée par le justificatif.

### Rencontrez Martin

La vidéo suivante se penche sur quelques-uns de ces concepts fondamentaux : identifiants, attributs, identité, autodéclaration, validation et vérification. L'identité objective, ou l'identité établie en liant des identifiants et des attributs à une personne/entité, est également un concept important.

Comme indiqué, l'identité peut s'appliquer à de nombreux types d'entités différentes. Certains de ces concepts sont illustrés en suivant *Martin* durant une journée typique.

<<Martin Explainer video goes here>>

### Vérifiez votre compréhension

Prenons un moment pour vérifier que vous avez bien compris les concepts que nous avons abordés jusqu'à présent. Dans cette activité, sélectionnez le terme approprié correspondant à la définition indiquée. Cette activité n'est pas chronométrée, alors n'hésitez pas à prendre votre temps pour la réaliser.

1. \_\_\_\_\_\_\_\_\_\_\_ prouvent tout, allant de l'éducation à l'autorisation de conduire un véhicule à moteur.
   1. \*Les justificatifs
   2. Les identifiants
   3. Les authentifiants
   4. Les attributs
2. \_\_\_\_\_\_\_\_\_\_\_ sont des représentations électroniques des assertions d'une identité ou des attributs de cette identité.
   1. Les identifiants
   2. Les authentifiants
   3. Les attributs
   4. \*Les justificatifs numériques
3. Nous appelons tout ce qui peut être identifié dans un contexte spécifique \_\_\_\_\_\_\_\_\_\_\_
   1. Un justificatif
   2. \*Une entité
   3. Une personne
   4. Un représentant
4. \_\_\_\_\_\_\_\_\_ sont nommé(e)s pour agir au nom d'une organisation.
   1. Les justificatifs
   2. Les entités
   3. Les personnes
   4. \*Les représentants
5. \_\_\_\_\_\_\_\_\_\_\_ est un élément sous le contrôle du sujet d'un justificatif numérique qui lui permet d’affirmer que l'identité numérique est la sienne.
   1. Un identifiant
   2. \*Un authentifiant
   3. Un attribut
   4. Un justificatif numérique
6. \_\_\_\_\_\_\_\_\_ permet, par exemple à la banque, de faire référence à l'identité numérique de manière unique.
   1. \*Un identifiant
   2. Un attribut
   3. Un lien
   4. Un sujet
7. Un justificatif numérique contient tous les éléments suivants, sauf lequel?
   1. Identifiant
   2. Attribut
   3. Lien
   4. \*Sujet
8. Chaque fois qu'une identité est prétendue par quelqu'un ou quelque chose, il y a un(e) \_\_\_\_\_\_\_\_.
   1. \*assertion
   2. lien
   3. attribut
   4. identifiant
9. \_\_\_\_\_\_\_\_\_ est le processus qui consiste à confirmer l'exactitude des informations présentées.
   1. Lier
   2. \*La validation
   3. L’autodéclaration
   4. La vérification
10. \_\_\_\_\_\_\_\_\_\_ est le processus qui consiste à confirmer que l'identité prétendue appartient de manière unique à l'entité qui la prétend.
    1. Lier
    2. La validation
    3. L’autodéclaration
    4. \*La vérification

## Création d'un justificatif numérique

### Cycle de vie des justificatifs numériques

Regardons maintenant le cycle de vie d’un justificatif numérique, de sa création à sa « mort ». En cours de route, nous introduisons quelques concepts supplémentaires liés aux justificatifs numériques.

Pour ceux d'entre vous qui sont plus exposés aux justificatifs numériques et aux standards associés pour la fourniture de services en ligne sécurisés, il existe une énorme quantité d’informations sur le processus et sur les définitions des composants de création et d'utilisation des justificatifs numériques. Nous allons utiliser une approche plus simplifiée pour présenter les concepts clés.

À un niveau avancé, le cycle de vie d'un justificatif numérique consiste communément en trois phases, de l'existence initiale d'une identité jusqu’à son utilisation, telle que représentée par un justificatif numérique. Ces phases sont :

1. L'existence initiale d'une identité ou d'une **entité** identifiable – Ceci peut se produire par la naissance d'une personne ou la constitution d'une entreprise. Il s'agit essentiellement de l'arrivée dans ce monde de quelqu’un, ou de quelque chose, à qui une identité peut être attribuée. Il ne s'agit pas encore d'une identité numérique.
2. Création et délivrance d'un justificatif numérique - On parle alors de **délivrance** ou **d'inscription**. La délivrance consiste en un ensemble de processus nécessaires à la création d'un justificatif numérique. Ce justificatif est le fondement qui permet une assertion d'identité.
3. Utilisation d'un justificatif numérique - Nous utiliserons le terme « **authentification** ». L'authentification est souvent conçue comme le processus consistant à fournir un **authentifiant** pour *se connecter*. Ici, nous considérons que l'authentification comprend le processus intégral de vérification d'un justificatif numérique dans le but d'obtenir l'accès et la permission d'effectuer une transaction.

En plus des phases du cycle de vie mentionnées ci-dessus, et selon les règles de gouvernance et de processus en place concernant le justificatif numérique, un justificatif numérique peut exister dans un certain nombre d'autres états. Par exemple, un justificatif numérique peut être révoqué et rendu inutilisable.

### Le processus de création d'un justificatif numérique

**Il existe de nombreuses approches pour créer un justificatif numérique, et ces processus varient en fonction des besoins et des préférences du créateur d'un justificatif numérique.** Certaines méthodes peuvent dépendre des préférences en matière de technologie ou de processus d’affaires. De même, le niveau de confiance requis lorsqu'on se fie au justificatif numérique aura une incidence importante sur les méthodes utilisées. Cependant, dans tous les cas, il existe des caractéristiques communes telles que :

1. l’assertion d’identité;
2. la production de preuve;
3. l'examen des preuves;
4. la création de justificatifs d'identité.

**Création d'un justificatif numérique (délivrance)**

Plus tôt, nous avons défini la **délivrance** comme l'ensemble des processus nécessaires pour délivrer un justificatif numérique. La délivrance, telle qu'utilisée ici, consiste en plusieurs processus distincts que nous allons examiner de plus près.

Veuillez noter qu'avant de procéder à la délivrance, l'organisation responsable de la création d'un justificatif numérique (appelons-la l'**émetteur**) doit d'abord formaliser son processus en fonction de l'utilisation prévue du justificatif numérique créé. Cela implique de se poser des questions telles que : « quelles preuves vais-je accepter? », « de qui vais-je les accepter? » et « quel est mon processus de validation et de vérification de ces preuves? ». Ceci est important pour s'assurer que le processus d'inscription s'aligne bien sur l'usage prévu et n'expose ni celui qui présente un justificatif numérique (la personne ou l'organisation à laquelle le justificatif numérique est lié) ni celui qui accepte un justificatif numérique (la personne ou l'organisation qui s'appuie sur le justificatif numérique pour la fourniture de services) à un risque indu.

Les activités précises et le niveau de vérification diligente varieront considérablement en fonction de l'utilisation prévue. Par exemple, un justificatif numérique créé pour des médias sociaux ou des jeux en ligne a des processus de validation et de vérification sensiblement différents de ceux d'un justificatif créé pour effectuer des transactions financières en ligne.

**La délivrance en action**

Maintenant que le processus est défini, examinons les éléments qui le composent en action. Plus tôt, nous avons défini quatre étapes de base dans le processus de délivrance. Examinons-les de plus près, ainsi que certaines des méthodes utilisées en fonction du contexte et de l'utilisation prévue du justificatif numérique.

Voici une illustration de la délivrance en action. Nous allons couvrir chacune de ces 4 étapes une par une :

[authentication cartoon here](https://docs.google.com/presentation/d/1M1405CpKI1wqggJObbdJMJajnGSdEAwK76wgU3MEsZ8/edit#slide=id.gc33538400f_0_0)

1. **L'assertion**

Le processus commence par une assertion de base de la part de la personne ou de l'organisation qui souhaite obtenir un justificatif numérique. Cela peut être aussi simple que « Je veux être MEGASTRIKER, le fanatique des jeux en ligne», ou quelque chose de plus précis comme « Je suis Marie Unetelle d’Halifax, et je veux déclarer mes impôts en ligne ». En d'autres termes, il devrait y avoir une intention déclarée de la part d'une personne ou d'une organisation de faire en sorte qu'une identité du « monde réel », pour laquelle elle a initialement fourni une autodéclaration d’identité, se reflète sous la forme d’un justificatif numérique.

1. **La production de preuves**

Selon le processus défini par l'émetteur, des preuves de l'identité prétendue seront requises. L'entité qui fait l'assertion ou les assertions doit produire des preuves pour les appuyer. À ce stade, l'émetteur suivra les processus qu'il juge nécessaires pour s'assurer que les preuves sont complètes et semblent provenir de sources acceptables.

En pratique, il peut s'agir d'une ou de plusieurs autodéclarations du sujet du justificatif numérique proposé (niveaux d'assurance les plus bas), de la production de preuves sous le contrôle du sujet (par exemple: permis de conduire, certificat de naissance, passeport) et/ou du consentement du sujet à consulter d'autres émetteurs de justificatifs numériques de confiance.

1. **Examen des preuves**

Dans cette phase de délivrance, les preuves acceptées sont évaluées pour déterminer si une identité numérique peut être créée. Cet examen comporte de nombreux éléments clés qui doivent être identifiés, entre autres par les questions auxquelles ils répondent :

- « Les preuves présentées sont-elles exactes? ». C'est la **validation** telle que nous l'avons définie précédemment. Ce processus peut prendre de nombreuses formes. Pour les justificatifs numériques destinés à être utilisés avec des niveaux de confiance moins élevés, il peut simplement reposer sur des autodéclarations et assurer un certain niveau de cohérence avec les preuves présentées. Cependant, pour les cas que nous voulons le plus explorer, ceux qui nécessitent des niveaux d'assurance plus élevés, le processus consiste généralement à s’assurer que:

- toutes les assertions de l'utilisateur correspondent aux informations enregistrées pour tous les éléments de preuve présentés (par exemple, s'il y a une assertion selon laquelle l'utilisateur a 40 ans, la date de naissance figurant sur un passeport présenté correspond-elle à cette assertion?).

- les preuves présentées proviennent de la source d'origine et n'ont pas été altérées. Dans les cas de niveau d'assurance inférieur, il peut être jugé suffisant que les preuves soient examinées par un examinateur qualifié. Pour les niveaux d'assurance plus élevés, une consultation avec l'autorité émettrice est souvent requise.

- la validation, si elle comprend une validation numérique avec un autre émetteur, soit soumise à des méthodes technologiques appropriées pour garantir que la communication entre émetteurs est infalsifiable et vérifiable.

- « Cette preuve est-elle liée au sujet? ». C'est la **vérification** telle que nous l'avons définie précédemment. Les méthodes employées sont les mêmes que celles utilisées pour la **validation**. En plus de s'assurer de l'exactitude des preuves présentées, l'émetteur doit vérifier que les informations, ou les identifiants présentés comme preuves, peuvent être associés de manière *unique* à la personne ou à l'organisation qui demande la création d'une identité numérique.

- « Sur la base de la politique de l'émetteur et des preuves présentées, puis-je créer un justificatif numérique qui correspondra à une entité unique? ». C'est ce qu'on appelle la **résolution**. La résolution est le processus qui consiste à établir que le sujet du justificatif numérique peut être décrit de manière à être unique dans l'ensemble des justificatifs numériques délivrés.

1. **La création d’un justificatif**

L'étape finale est la création du justificatif numérique qui facilite l'utilisation d'une identité numérique - Avec un examen réussi des preuves, le justificatif numérique peut être créé. Plus tôt, nous avons défini deux termes qui seront importants lorsque nous examinerons la création d'une identité numérique et son utilisation subséquente : le **justificatif d'identité** (la somme totale des informations des assertions et des identifiants enregistrés aux fins du justificatif numérique) et l'**authentifiant** (un artefact physique ou numérique utilisé le plus souvent pour faciliter l'authentification).

**Utilisation d'un justificatif numérique**

Voyons maintenant un justificatif numérique en action. Lors de la **délivrance**, nous créons un **justificatif** numérique et un **authentifiant**. Le justificatif numérique est prêt à être utilisé, ce que nous avons défini comme une **authentification**.

Examinons un exemple d'utilisation de l'identité avec certains éléments d'assertions contenus dans un justificatif numérique.

1. À l'aéroport, vous vous enregistrez et obtenez votre carte d'embarquement, puis vous vous dirigez vers la zone d'embarquement.
2. Avant d'être autorisé à entrer dans la zone d'embarquement, on vous demande votre carte d'embarquement et une pièce d'identité délivrée par le gouvernement (vous utilisez votre passeport). L'agent vérifie que les informations de la carte d'embarquement (nom, etc.) correspondent à celles indiquées sur le passeport [**validation**] et que la photo sur le passeport vous ressemble [**vérification**].
3. En outre, un scanneur lit les informations électroniques contenues dans le passeport et les affiche à l'agent, ce qui lui permet de s'assurer que le passeport n'a pas été falsifié [**vérification**].
4. De plus, selon l'aéroport et le pays où vous vous trouvez, il peut y avoir une interaction sécurisée entre systèmes avec le bureau des passeports pour vérifier si le passeport est valide [**vérification**].

Les informations enregistrées au bureau des passeports constituent le **justificatif d’identité** complet. Une partie ou l'ensemble des informations du justificatif d’identité peuvent avoir été incluses dans les informations imprimées et électroniques intégrées au passeport, et le passeport physique lui-même sert d'**authentifiant**.

### Plus d'informations sur la création d'un justificatif numérique

Enfin, une brève introduction à certains termes supplémentaires que nous utiliserons tout au long de ce programme d'apprentissage.

Il existe différents types de justificatifs et de preuves d’assertions. Les preuves fondamentales reposent sur des événements fondamentaux basés sur des faits qui peuvent être utilisés pour établir un justificatif **fondamental**. De bons exemples sont la naissance ou l'immigration pour les personnes, et la constitution en société pour une entité commerciale enregistrée. Les justificatifs numériques **contextuels** sont utilisés dans un but précis, dans un contexte précis. Parmi les exemples de justificatifs contextuels et des preuves associées, on peut citer les justificatifs d’identité bancaires, les permis de conduire, ou même quelque chose d'aussi simple qu'un compte valide sur les médias sociaux.

Enfin, dans les sections ultérieures de ce programme d'apprentissage, nous nous penchons sur le risque associé à l'utilisation d’un justificatif numérique, la confiance dans un justificatif et les **niveaux d'assurance**. Intuitivement, nous comprenons que l'utilisation des justificatifs d'une personne sur les médias sociaux donne moins confiance au fait que cette personne est bien celle qu'elle prétend être, surtout comparativement à un permis de conduire valide, délivré par le gouvernement. En général, il existe des **niveaux d'assurance** formellement définis qui servent d'indicateurs relativement au degré de confiance que l'on peut avoir dans un justificatif numérique. Cela aide les créateurs et les consommateurs d'un justificatif numérique à définir les **fournisseurs** **de confiance** en matière d'identité ou de preuves d'identité qui conviennent au contexte du service électronique offert.

### Rencontrez Susan

Essayons de relier tout cela en illustrant le cycle de vie d'un justificatif numérique, et certains de nos concepts définis, dans un scénario où une entreprise souhaite s'inscrire à la déclaration d’impôt en ligne en utilisant son comptable comme **représentant**. La délivrance s'appuiera sur des preuves **fondamentales** et **contextuelles** dans un contexte qui exige un **niveau d'assurance** relativement élevé.

<<Susan Explainer video goes here>>

### Vérifiez votre compréhension

Prenons un moment pour vérifier que vous avez bien compris les concepts que nous avons abordés jusqu'à présent. Dans cette activité, sélectionnez le terme approprié correspondant à la définition indiquée. Cette activité n'est pas chronométrée, alors n'hésitez pas à prendre votre temps pour la réaliser. Vous ne disposez que d'une seule tentative.

1. le cycle de vie d'une identité numérique consiste communément en \_\_\_\_ phases, de l'existence initiale d'une identité jusqu’à son utilisation, telle que représentée par un justificatif numérique.
   1. un
   2. deux
   3. \*trois
   4. quatre
2. Il existe de nombreuses approches pour créer un justificatif numérique, et ces processus varient en fonction des besoins et des préférences du créateur d'un justificatif numérique.
   1. \*Vrai
   2. Faux
3. Le processus de délivrance comporte \_\_\_ étapes de base.
   1. un
   2. deux
   3. trois
   4. \*quatre
4. Le processus de délivrance commence par
   1. L'examen des preuves
   2. \*Une assertion
   3. La production de preuves
   4. La création d'un justificatif
5. La dernière étape du processus de délivrance est
   1. L'examen des preuves
   2. Une assertion
   3. La production de preuves
   4. \*La création d'un justificatif
6. Le justificatif numérique est souvent utilisé pour
   1. \*l'authentification
   2. un justificatif
   3. la délivrance
   4. la vérification
7. Parmi les exemples de justificatifs contextuels et des preuves associées, on peut citer les justificatifs d’identité bancaires et les permis de conduire.
   1. \*Vrai
   2. Faux
8. « Les preuves présentées sont-elles exactes? » Il s'agit d'un exemple de :
   1. Délivrance
   2. Vérification
   3. \*Validation
   4. Aucune de ces réponses

## Entrevues avec des experts

### Entrevue avec Patrick Drolet

Nous sommes très heureux de pouvoir faire appel à certains des experts reconnus dans le paysage canadien de l'identité numérique pour nous aider dans ce programme éducatif. Dans cette courte entrevue, nous parlons avec Patrick Drolet, Vice-président des opérations et de la stratégie de produit pour Notarius, de la validation, de la vérification et de certaines des questions critiques liées aux justificatifs numériques que nous explorerons plus en détail au fur et à mesure de notre parcours d'apprentissage. Patrick présente certains des principaux obstacles à l'adoption et à l'utilisation des justificatifs numériques, ainsi que certains des développements intéressants qui permettront de surmonter ces obstacles.

<<Patrick Drolet interview goes here>>

## Conclusion

Nous espérons que cette introduction au monde des justificatifs numériques servira de base aux modules d'apprentissage à venir. Elle permettra certainement de clarifier la terminologie utilisée lorsque les gens parlent de justificatifs numériques.

Cette introduction aborde les principaux composants des justificatifs numériques et discute de certains termes clés dans un domaine complexe. Dans les modules d'apprentissage à venir, nous introduirons des concepts qui s'appuient sur les termes présentés ici pour comprendre comment les justificatifs numériques sont créés, gérés et utilisés.

## Questionnaire du module 1

Vous n'avez qu'un seul essai pour répondre à ce questionnaire sur le module comportant dix-neuf (19) questions. Ce questionnaire n'est pas chronométré, alors prenez votre temps pour examiner attentivement les choix de réponses. Vous avez un seul essai.

1. Un/une \_\_\_\_\_\_\_\_\_\_est un indicateur qui pointe vers une personne déterminée. Il peut être unique dans un système défini, comme le numéro d'assurance sociale (NAS) au Canada.
   1. (Identifiant)
   2. Attribut
   3. Identité
   4. Validation
2. Un/une \_\_\_\_\_\_\_\_\_\_ est une propriété susceptible d'être partagée par de nombreuses personnes. Ils/elles peuvent être professionnels (par exemple: avocat, CPA, ingénieur, architecte). Ils/elles peuvent également être des affiliations (par exemple: employé d'une entreprise, membre d'une association d'anciens étudiants), des caractéristiques physiques (par exemple: couleur des yeux, sexe, taille), ou être en rapport avec la taille d'une entreprise (par exemple: petite et moyenne).
   1. Identifiant
   2. (Attribut)
   3. Identité
   4. Validation
3. Un/une \_\_\_\_\_\_\_\_\_\_ est une représentation dequi vous prétendez être et de qui vous êtes.
   1. Authentifiant
   2. Inscription
   3. (Identité)
   4. Identifiant
4. La validation confirme l'exactitude des informations présentées, tandis que la vérification assure qu'elles appartiennent à l'entité à laquelle s'applique l'assertion d'identité.
   1. (Vrai)
   2. Faux
5. Les caractéristiques de l'identité peuvent être trouvées dans un \_\_\_\_\_\_\_\_\_\_\_\_\_\_.
   1. (justificatif d’identité)
   2. niveau d’assurance
   3. vérification
   4. validation
6. S'assurer que toutes les preuves d'identité présentées sont cohérentes fait partie de la/de l’ \_\_\_\_\_\_\_\_\_\_\_
   1. Authentification
   2. Résolution
   3. (validation)
   4. Possession
7. Lorsque l'agent des services frontaliers vérifie la photo sur votre passeport pour s'assurer qu'elle vous ressemble, il s'agit d'un exemple de/d’ \_\_\_\_\_\_\_\_\_\_\_
   1. (vérification)
   2. niveau d’assurance
   3. résolution
   4. identification
8. Votre nom d'utilisateur est un exemple de/d’ \_\_\_\_\_\_\_\_\_\_\_\_\_
   1. (identifiant)
   2. inscription
   3. authentifiant
   4. justificatif d’identité
9. Lorsque vous dites votre nom à quelqu'un, cela s'appelle un authentifiant.
   1. Vrai
   2. (faux)
10. Les preuves d'identité qui ne sont pas fondamentales sont appelées des preuves d'identité \_\_\_\_\_\_\_\_\_\_\_.
    1. (contextuelle)
    2. de possession
    3. authentique
    4. Elles sont toujours fondamentales
11. La première phase du cycle de vie d'un justificatif numérique est:
    1. La création et la délivrance d'un justificatif numérique (délivrance ou inscription)
    2. L'utilisation d'un justificatif numérique (authentification)
    3. \*L'existence initiale d'une identité (entité identifiable)
    4. La fin d'un justificatif numérique (sa «mort»)
12. La deuxième phase du cycle de vie d'un justificatif numérique est:
    1. \*La création et la délivrance d'un justificatif numérique (délivrance ou inscription)
    2. L'utilisation d'un justificatif numérique (authentification).
    3. L'existence initiale d'une identité (entité identifiable)
    4. La fin d'un justificatif numérique (sa «mort»)
13. La troisième phase du cycle de vie d'un justificatif numérique est:
    1. La création et la délivrance d'un justificatif numérique (délivrance ou inscription)
    2. \*L'utilisation d'un justificatif numérique (authentification).
    3. L'existence initiale d'une identité (entité identifiable)
    4. La fin d'un justificatif numérique (sa «mort»)
14. Veuillez noter qu'avant de procéder à la délivrance, l'organisation responsable de la création d'un justificatif numérique doit d'abord formaliser son processus en fonction de l'utilisation prévue du justificatif numérique créé. Cela implique de se poser des questions telles que : « quelles preuves vais-je accepter? »
    1. \*Vrai
    2. Faux
15. La divulgation de votre nom et de votre emplacement fait généralement partie de quelle étape du processus de délivrance?
    1. L'examen des preuves
    2. \*L’assertion
    3. La création d'un justificatif
    4. La production de preuves
16. L'examen des preuves d'assertion d'identité pour s'assurer qu'elles sont complètes et semblent provenir de sources acceptables est généralement effectué à quelle étape du processus de délivrance des justificatifs?
    1. L'examen des preuves
    2. L’assertion
    3. La création d'un justificatif
    4. \*La production de preuves
17. « Les preuves présentées sont-elles exactes? », « Cette preuve est-elle liée au sujet? », ou « Sur la base de la politique de l'émetteur et des preuves présentées, puis-je créer un justificatif numérique qui correspondra à une entité unique? » sont des questions qui sont généralement posées au cours de quelle phase du processus de délivrance ?
    1. \*L'examen des preuves
    2. L’assertion
    3. La création d'un justificatif
    4. La production de preuves
18. Cette dernière étape du processus de délivrance facilite l'utilisation d'une identité numérique.
    1. L'examen des preuves
    2. L’assertion
    3. \*La création d'un justificatif
    4. La production de preuves
19. Il n'existe qu'un seul type de justificatif et de preuves des assertions.
    1. Vrai
    2. \*Faux

### 

# 

# Module 2 : Concepts relatifs aux justificatifs numériques

## Introduction

Dans le module d'apprentissage précédent, nous avons défini certains des termes fondamentaux utilisés lors de l'exploration du monde des justificatifs numériques. Dans ce module, nous définirons certains des concepts et des termes clés employés lorsque nous examinons la conception des systèmes et des processus utilisés pour créer et échanger des justificatifs numériques.

Objectifs d'apprentissage

1. Examiner les facteurs d'authentification et l'authentification multifacteur
2. Apprendre les concepts clés concernant les justificatifs numériques

## Facteurs d'authentification et authentification multifacteur

Plus tôt, nous avons défini un authentifiant comme un élément sous le contrôle du **sujet** d'un justificatif numérique qui lui permet d'affirmer que le justificatif numérique est le sien. De quoi s'agit-il? À quoi ressemble-t-il?

Un authentifiant peut être :

* Quelque chose que vous connaissez. Les plus courants sont les mots de passe, les NIP, ou même les réponses à des questions d'identification préconfigurées.
* Quelque chose que vous avez. Il peut s'agir, par exemple, d'une carte à puce ou d'une carte d'accès, de votre téléphone intelligent ou d'un autre type de jeton physique utilisé pour avoir accès à quelque chose.
* Quelque chose que vous êtes. Souvent, il s'agit d'une caractéristique biométrique, comme une empreinte digitale ou une analyse rétinienne.

Récemment, vous avez peut-être entendu le terme « authentification à deux facteurs » ou « authentification multifacteur ». De plus en plus de fournisseurs de services en ligne implémentent des processus qui requièrent plus d'un authentifiant afin de fournir un niveau de sécurité supplémentaire. Par exemple, l'utilisation de votre téléphone ou de votre compte de messagerie pour vous envoyer un NIP à usage unique à utiliser pour compléter votre connexion auprès du fournisseur de services. Dans ce scénario, vous fournissez votre mot de passe (quelque chose que vous connaissez) et vous êtes ensuite informé qu'un NIP à usage unique a été envoyé à votre adresse électronique. Vous récupérez le NIP, vous le saisissez et vous obtenez ensuite l'accès. En fait, cela combine un élément supplémentaire que vous connaissez (le NIP) avec un élément que vous avez (votre compte de messagerie).

Ces facteurs d'authentification, ou authentifiants, sont souvent classés comme suit :

* facteurs de connaissance (c'est-à-dire quelque chose que vous savez)
* facteurs de possession (c'est-à-dire quelque chose que vous avez)
* facteurs biométriques (c'est-à-dire quelque chose que vous êtes)

### Rencontrer Natalie

Penchons-nous à nouveau sur l'authentification en action. La vidéo ci-dessous nous montre le processus pour accéder à votre compte fiscal en utilisant un fournisseur d'identité de confiance, votre banque, pour donner accès au service fiscal.

<<Natalie Explainer video goes here>>

## Concepts importants relatifs aux justificatifs numériques

### Introduction

Les termes qui suivent définissent un certain nombre de concepts clés qui sont importants dans les méthodes centrées sur l'utilisateur pour la délivrance et l'utilisation de justificatifs numériques qui renforcent la protection de la vie privée, sont contrôlés par l'utilisateur et sont plus sécurisés. Dans ce module d'apprentissage, nous définirons brièvement ces termes et les explorerons plus en détail lorsque nous examinerons certaines des approches en matière de processus et de technologie pour la gestion des justificatifs numériques.

### Justificatifs vérifiables

Au niveau le plus simple, les justificatifs numériques ne sont rien d'autre que l'équivalent électronique des justificatifs physiques que nous utilisons déjà aujourd'hui : cartes de crédit, passeports, permis de conduire et des choses comme des compétences et des reconnaissances. Les justificatifs vérifiables, tels que nous les décrirons dans ce programme d'apprentissage, impliquent un modèle particulier pour la délivrance et l'utilisation d'un justificatif numérique. Nous y reviendrons plus en détail dans les modules d'apprentissage suivants.

Le [W3C](https://www.w3.org/TR/vc-data-model/) définit les justificatifs vérifiables comme [*un mécanisme permettant d'exprimer les justificatifs d'identité sur le Web d'une manière qui est cryptographiquement sécurisée, qui respecte la vie privée et qui est vérifiable de façon automatisée*](https://www.w3.org/TR/vc-data-model/) *(traduit de l’anglais)*. Les justificatifs vérifiables peuvent être utilisés pour établir la confiance entre les parties en utilisant un ensemble d’assertions et de métadonnées inviolables qui prouvent de manière cryptographique l'identité du titulaire et de son émetteur. Plus important encore, en utilisant cette approche, les utilisateurs peuvent conserver leurs données et simplement partager les informations nécessaires sous la forme d'un justificatif vérifié avec une autre partie lorsqu'ils reçoivent une demande. Les justificatifs vérifiables présentent les avantages suivants : le justificatif fournit une preuve cryptographique que le document est authentique, que les informations n'ont pas été altérées, ainsi qu'une méthode d'authentification forte de l'émetteur sans que celui-ci ait à participer à l'échange.

### Identifiants décentralisés

Lorsque nous définissons les justificatifs vérifiables et les caractéristiques générales des modèles d'écosystèmes pour la délivrance et l'utilisation d'un justificatif vérifiable, nous notons que le justificatif est sous le contrôle du titulaire de ce justificatif et que son utilisation ne doit pas impliquer l'émetteur de ce justificatif de quelque manière que ce soit. Pour ce faire, il doit exister une méthode permettant la vérification cryptographique et la preuve de l'authenticité d'un justificatif vérifiable, sans avoir à consulter l'émetteur de ce justificatif numérique. Ces deux caractéristiques importantes (c'est-à-dire le contrôle du justificatif par le titulaire et l'utilisation d'un justificatif sans consultation de l'émetteur) ont conduit au développement de modèles pour la gestion des justificatifs numériques qui sont décentralisés - la propriété et le stockage des justificatifs sous le contrôle direct des individus à qui les justificatifs numériques sont délivrés, et l'élimination de la nécessité de consulter une autorité centralisée lorsqu'un justificatif est utilisé.

Il est donc nécessaire que les vérificateurs d'un justificatif vérifiable soient en mesure de comprendre comment authentifier un justificatif et son titulaire, et de s'assurer de l'origine d'un justificatif. Les identifiants décentralisés (DID) sont des identifiants uniques qui pointent vers les documents des identifiants décentralisés (*DID documents*) qui contiennent les clés publiques, et identifient les méthodes qui seront nécessaires pour valider l'authenticité d'un justificatif vérifiable.

### Registre distribué

Un composant important des modèles décentralisés est le composant du système où sont stockés les documents des identifiants décentralisés (*DID documents*) et les autres informations disponibles nécessaires à la vérification d'un justificatif numérique. Il peut s'agir de toute base de données partagée de manière consensuelle, synchronisée et accessible sur plusieurs sites. Il n'y a pas de format de base de données prescrit ou de technologie requise pour un registre distribué, il suffit qu'il soit disponible à grande échelle dans l'écosystème au sein duquel un justificatif numérique est délivré et utilisé. Cependant, le plus souvent, dans les systèmes d'identité numérique disponibles dans le monde entier, ces registres distribués sont mis en œuvre à l'aide de la technologie de la chaîne de blocs (*blockchain*).

### Vérifiez votre compréhension

Prenons un moment pour vérifier que vous avez bien compris les concepts que nous avons abordés jusqu'à présent. Dans cette activité, sélectionnez le terme approprié correspondant à la définition indiquée. Cette activité n'est pas chronométrée, alors n'hésitez pas à prendre votre temps pour la réaliser.

1. \_\_\_\_\_\_\_ peut/peuvent être quelque chose que vous savez, quelque chose que vous avez ou quelque chose que vous êtes.
2. Les justificatifs vérifiables
3. L’authentification multifacteur ou à deux facteurs
4. \*Un authentifiant
5. Un registre distribué
6. Les identifiants décentralisés
7. Un exemple de ceci est l'utilisation de votre téléphone ou de votre compte de messagerie pour vous envoyer un NIP à usage unique à utiliser pour compléter votre connexion auprès du fournisseur de services.
8. Justificatifs vérifiables
9. \*Authentification multifacteur ou à deux facteurs
10. Authentifiant
11. Registre distribué
12. Identifiants décentralisés
13. \_\_\_\_\_\_\_\_ est/sont un mécanisme permettant d'exprimer les justificatifs d'identité sur le Web d'une manière qui est cryptographiquement sécurisée, qui respecte la vie privée et qui est vérifiable de façon automatisée.
14. \*Les Justificatifs vérifiables
15. L’authentification multifacteur ou à deux facteurs
16. Un authentifiant
17. Un registre distribué
18. Les identifiants décentralisés
19. \_\_\_\_\_\_\_\_\_\_ sont des identifiants uniques qui pointent vers les documents des identifiants décentralisés (*DID documents*) qui contiennent les clés publiques, et identifient les méthodes qui seront nécessaires pour valider l'authenticité d'un justificatif vérifiable.
20. Les justificatifs vérifiables
21. Les authentifications multifacteurs ou à deux facteurs
22. Les authentifiants
23. Les registres distribués
24. \*Les identifiants décentralisés
25. Il n'y a pas de format de base de données prescrit ou de technologie requise pour \_\_\_\_\_\_\_\_\_\_, il suffit qu'il/elle/ils soit/soient disponible(s) à grande échelle dans l'écosystème au sein duquel un justificatif numérique est délivré et utilisé.
26. les justificatifs vérifiables
27. l’authentification multifacteur ou à deux facteurs
28. un authentifiant
29. \*un registre distribué
30. les identifiants décentralisés

### Portefeuilles numériques

Un portefeuille numérique est un outil technologique conçu pour contenir vos justificatifs numériques. Il est important de noter que les portefeuilles numériques utilisés pour les justificatifs numériques diffèrent des portefeuilles plus spécialisés conçus à des fins financières précises (cryptomonnaies, systèmes de paiement tels que Apple Pay ou Google Pay, etc.) Un portefeuille numérique permet au titulaire d'un justificatif numérique d'interagir avec des émetteurs ou des vérificateurs de justificatifs numériques pour échanger des justificatifs de manière fiable.

### Identité auto-souveraine

L'identité auto-souveraine (IAS) est un modèle de justificatifs numériques qui repose sur un certain nombre de concepts clés permettant de créer une approche respectueuse de la vie privée et centrée sur l'utilisateur pour la délivrance et l'utilisation des justificatifs numériques. Dans le cas des justificatifs physiques que vous portez sur vous, c'est le titulaire du justificatif qui décide avec qui il le partage et dans quel but. Grâce à l'existence de moyens standardisés pour exprimer un justificatif (justificatifs vérifiables), d'approches standardisées pour permettre l'utilisation d'un justificatif numérique (identifiants décentralisés et registres distribués), et du stockage de justificatifs numériques contrôlé par l'utilisateur (portefeuilles numériques), il est possible d'avoir un modèle dans lequel l'utilisateur a le contrôle de son justificatif numérique.

Les caractéristiques de l'IAS comprennent le contrôle direct et exclusif des justificatifs numériques par l'utilisateur, la possibilité de décider au cas par cas ce qui est partagé et à quel titre, et la possibilité d'utiliser un justificatif vérifiable sans avoir à consulter l'émetteur de ce justificatif pour vérifier son authenticité.

Dans les modules d'apprentissage ultérieurs, nous explorerons l'IAS plus en détail.

### Divulgation sélective

Dans le prolongement du modèle de l'IAS, il existe un concept de divulgation sélective selon lequel seules les informations minimales requises sont partagées avec un vérificateur de justificatifs. Un élément important de la protection renforcée de la vie privée, et de nombreuses lois sur la protection de la vie privée en vigueur, consiste à limiter les renseignements personnels partagés à ce qui est nécessaire à la réalisation de la transaction.

Le concept de divulgation sélective, appliqué à l'utilisation des justificatifs numériques, implique que les utilisateurs devraient pouvoir choisir ce qu'ils partagent et dans quelle mesure, au cas par cas. La disponibilité d'outils et de techniques permettant l'IAS (justificatifs vérifiables, identifiants distribués, portefeuilles d'identité numérique, etc.) fournit une base pour étendre la capacité des portefeuilles numériques et des outils utilisés par les vérificateurs qui reçoivent des justificatifs numériques de demander et partager uniquement les informations requises pour une transaction déterminée.

Prenons un exemple concret : lorsqu'une personne fournit son permis de conduire pour prouver son âge, le vérificateur d'un justificatif de permis de conduire physique voit également l'adresse du fournisseur (ou du titulaire) du justificatif. Cette information n'est pas nécessaire pour prouver l'âge et constitue une violation des principes relatifs à la protection de la vie privée. Grâce à la divulgation sélective, qui fait appel à des techniques cryptographiques avancées, le vérificateur ne reçoit que la date de naissance du justificatif numérique.

### Preuve à divulgation nulle de connaissance

La preuve à divulgation nulle de connaissance étend le concept de l'IAS encore plus loin, en fournissant des méthodes pour prouver la possession ou la connaissance d'un élément d'information sans divulguer la valeur réelle de cette information. Les exemples utilisés dans de nombreuses explications de la preuve à divulgation nulle de connaissance comprennent la preuve que votre date de naissance est supérieure à une certaine date (par exemple, «j'ai plus de 18 ans») ou que vous avez plus d'un certain montant dans un compte bancaire, sans révéler le montant exact du compte ou la date de naissance.

La preuve à divulgation nulle de connaissance repose sur une cryptographie à clé publique avancée, des calculs appliqués aux informations protégées et des méthodes de signature numérique pour créer une preuve cryptographique de la connaissance d'une information sans partager la valeur de cette information. Dans un module d'apprentissage ultérieur, nous approfondirons la preuve à divulgation nulle de connaissance et son fonctionnement. Outre les exemples cités ci-dessus, la preuve à divulgation nulle de connaissance promet de fournir une authentification «sans mot de passe», permettant à un utilisateur de prouver la possession d'un secret sans le partager (par exemple, «je peux prouver que je possède le mot de passe délivré et qu'il provient de l'émetteur, mais je n'ai pas besoin de vous l'envoyer et de l'exposer à des acteurs malveillants sur Internet»).

### Vérifiez votre compréhension

Prenons un moment pour vérifier que vous avez bien compris les concepts que nous avons abordés jusqu'à présent. Dans cette activité, sélectionnez le terme approprié correspondant à la définition indiquée. Cette activité n'est pas chronométrée, alors n'hésitez pas à prendre votre temps pour la réaliser.

1. \_\_\_\_\_\_\_\_\_\_\_ est un outil technologique conçu pour contenir vos justificatifs numériques.
   * La divulgation sélective
   * La preuve à divulgation nulle de connaissance
   * \*Un portefeuille numérique
   * L’identité auto-souveraine (IAS)
   * Un portefeuille d'identité numérique
2. \_\_\_\_\_\_\_\_\_\_\_ permet au titulaire d'un justificatif numérique d'interagir avec des émetteurs ou des vérificateurs de justificatifs numériques pour échanger des justificatifs de manière fiable.
   * La divulgation sélective
   * La preuve à divulgation nulle de connaissance
   * Un portefeuille numérique
   * L’identité auto-souveraine (IAS)
   * \*Un portefeuille d'identité numérique
3. \_\_\_\_\_\_\_\_\_\_\_ est un modèle de justificatifs numériques qui repose sur un certain nombre de concepts clés permettant de créer une approche respectueuse de la vie privée et centrée sur l'utilisateur pour la délivrance et l'utilisation des justificatifs numériques.
   * La divulgation sélective
   * La preuve à divulgation nulle de connaissance
   * Un portefeuille numérique
   * \*L’identité auto-souveraine (IAS)
   * Un portefeuille d'identité numérique
4. Le concept de \_\_\_\_\_\_\_\_\_\_\_, appliqué à l'utilisation des justificatifs numériques, implique que les utilisateurs devraient pouvoir choisir ce qu'ils partagent et dans quelle mesure, au cas par cas.
   * \*divulgation sélective
   * la preuve à divulgation nulle de connaissance
   * portefeuille numérique
   * l’identité auto-souveraine (IAS)
   * portefeuille d'identité numérique
5. \_\_\_\_\_\_\_\_\_\_\_\_\_\_ étend le concept de l'IAS encore plus loin, en fournissant des méthodes pour prouver la possession ou la connaissance d'un élément d'information sans divulguer la valeur réelle de cette information.
   * La divulgation sélective
   * \*La preuve à divulgation nulle de connaissance
   * Le portefeuille numérique
   * L’identité auto-souveraine (IAS)
   * Le portefeuille d'identité numérique

## Entrevues avec des experts

### Entrevue avec Andre Boysen

Nous sommes heureux d'avoir avec nous M. Andre Boysen, directeur de l'identité chez Securekey, pour nous parler des justificatifs et de certains des avantages importants que les innovations comme les justificatifs vérifiables nous apporteront. M. Boysen traite plus en détail des justificatifs et aide à introduire les sujets que nous explorerons dans les modules d'apprentissage ultérieurs (par exemple, la protection de la vie privée, la prévention de la fraude, la facilité d'utilisation, les avancées importantes en matière de technologie et de processus).

<<Andre Boysen interview to be inserted here>>

### Entrevue avec Mathieu Desrosiers

Nous avons le plaisir d'avoir avec nous M. Mathieu Desrosiers, responsable des services bancaires courants, des paiements et de l'identité numérique chez Desjardins. M. Desrosiers a pris le temps de nous parler de la relation entre les consommateurs et les entreprises en ce qui concerne l'identité numérique. M. Desrosiers parle des préoccupations des consommateurs, de la façon dont elles pourraient être atténuées, et de certaines des principales améliorations qui nous attendent.

<<Mathieu Desrosiers interview inserted here>>

## Conclusion

Les concepts clés que nous avons définis dans ce module d'apprentissage seront approfondis dans les modules suivants lorsque nous commencerons à explorer certaines des technologies et certains des standards utilisés dans la mise en œuvre des justificatifs numériques.

## Questionnaire du module 2

Choisissez la meilleure réponse dans le questionnaire à choix multiple portant sur les concepts de ce module d'apprentissage. Vous n'avez qu'une seule tentative pour ce questionnaire, mais prenez le temps dont vous avez besoin.

1. \_\_\_\_\_\_\_\_\_\_ présente/présentent les avantages suivants : le justificatif fournit une preuve cryptographique que le document est authentique, que les informations n'ont pas été altérées, ainsi qu'une méthode d'authentification forte de l'émetteur sans que celui-ci ait à participer à l'échange.
   1. \*Les justificatifs vérifiables
   2. L’authentification à deux facteurs ou multifacteur
   3. Les authentifiants
   4. Les modèles décentralisés
   5. Les justificatifs numériques
2. \_\_\_\_\_\_\_\_\_ est/sont souvent classé(s) comme suit : facteurs de connaissance, facteurs de possession, facteurs biométriques.
   1. Les justificatifs vérifiables
   2. L’authentification à deux facteurs ou multifacteur
   3. \*Les authentifiants
   4. Les modèles décentralisés
   5. Les justificatifs numériques
3. Un composant important \_\_\_\_\_\_\_\_ est le composant du système où sont stockés les documents des identifiants décentralisés (*DID documents*) et les autres informations disponibles nécessaires à la vérification d'un justificatif numérique.
   1. des justificatifs vérifiables
   2. de l’authentification à deux facteurs ou multifacteur
   3. des authentifiants
   4. \*des modèles décentralisés
   5. des justificatifs numériques
4. \_\_\_\_\_\_\_\_\_\_ implique/impliquent un modèle particulier pour la délivrance et l'utilisation d'un justificatif numérique.
   1. \*Les justificatifs vérifiables
   2. L’authentification à deux facteurs ou multifacteur
   3. Les authentifiants
   4. Les modèles décentralisés
   5. Les justificatifs numériques
5. Dans ce scénario, vous fournissez votre mot de passe (quelque chose que vous connaissez) et vous êtes ensuite informé qu'un NIP à usage unique a été envoyé à votre adresse électronique. Vous récupérez le NIP, vous le saisissez et vous obtenez ensuite l'accès.
   1. Les justificatifs vérifiables
   2. \*L’authentification à deux facteurs ou multifacteur
   3. Les authentifiants
   4. Les modèles décentralisés
   5. Les justificatifs numériques
6. Au niveau le plus simple, \_\_\_\_\_\_\_\_\_\_ n’est/ne sont rien d'autre que l'équivalent électronique des justificatifs physiques que nous utilisons déjà aujourd'hui : cartes de crédit, passeports, permis de conduire et des choses comme des compétences et des reconnaissances.
   1. Les justificatifs vérifiables
   2. L’authentification à deux facteurs ou multifacteur
   3. Les authentifiants
   4. Les modèles décentralisés
   5. \*Les justificatifs numériques
7. \_\_\_\_\_\_\_\_\_ peut/peuvent être utilisé(s) pour établir la confiance entre les parties en utilisant un ensemble d’assertions et de métadonnées inviolables qui prouvent de manière cryptographique l'identité du titulaire et de son émetteur.
   1. \*Les justificatifs vérifiables
   2. L’authentification à deux facteurs ou multifacteur
   3. Les authentifiants
   4. Les modèles décentralisés
   5. Les justificatifs numériques
8. Il doit exister une méthode permettant la vérification cryptographique et la preuve de l'authenticité d'un justificatif vérifiable, sans avoir à consulter l'émetteur de ce justificatif numérique. Ces deux caractéristiques importantes (c'est-à-dire le contrôle du justificatif par le titulaire et l'utilisation d'un justificatif sans consultation de l'émetteur) ont conduit au développement de modèles \_\_\_\_\_\_\_\_\_\_ pour la gestion des justificatifs numériques.
   1. de justificatifs vérifiables
   2. d’authentification à deux facteurs ou multifacteur
   3. d’authentifiants
   4. \*décentralisés
   5. de justificatifs numériques
9. Le plus souvent, dans les systèmes d'identité numérique disponibles dans le monde, nous voyons cette/ces \_\_\_\_\_\_\_\_\_\_ mis(e) en œuvre à l'aide de la technologie des chaînes de blocs.
   1. identité auto-souveraine (IAS)
   2. preuve à divulgation nulle de connaissance
   3. portefeuilles numériques
   4. \*registres distribués
   5. divulgation sélective
10. Il est important de noter que \_\_\_\_\_\_\_ utilisé(e)(s) pour les justificatifs numériques diffère/diffèrent des portefeuilles plus spécialisés conçus à des fins financières précises (cryptomonnaies, systèmes de paiement tels que Apple Pay ou Google Pay, etc.)
    1. l’identité auto-souveraine (IAS)
    2. la preuve à divulgation nulle de connaissance
    3. \*les portefeuilles numériques
    4. les registres distribués
    5. la divulgation sélective
11. Les caractéristiques de la/de l’/des \_\_\_\_\_\_\_\_\_ comprennent le contrôle direct et exclusif des justificatifs numériques par l'utilisateur, la possibilité de décider au cas par cas ce qui est partagé et à quel titre, et la possibilité d'utiliser un justificatif vérifiable sans avoir à consulter l'émetteur de ce justificatif pour vérifier son authenticité.
    1. \*identité auto-souveraine (IAS)
    2. preuve à divulgation nulle de connaissance
    3. portefeuilles numériques
    4. registres distribués
    5. divulgation sélective
12. \_\_\_\_\_\_\_\_\_ repose/reposent sur une cryptographie à clé publique avancée, des calculs appliqués aux informations protégées et des méthodes de signature numérique pour créer une preuve cryptographique de la connaissance d'une information sans partager la valeur de cette information.
    1. L’identité auto-souveraine (IAS)
    2. \*La preuve à divulgation nulle de connaissance
    3. Les portefeuilles numériques
    4. Les registres distribués
    5. La divulgation sélective
13. Dans le prolongement du modèle de l'IAS, il existe un concept de/d’ \_\_\_\_\_\_\_\_\_\_ selon lequel seules les informations minimales requises sont partagées avec un vérificateur de justificatifs.
    1. identité auto-souveraine (IAS)
    2. preuve à divulgation nulle de connaissance
    3. portefeuilles numériques
    4. registres distribués
    5. \*divulgation sélective
14. Les exemples utilisés dans de nombreuses explications de/des \_\_\_\_\_\_\_\_\_\_\_ comprennent la preuve que votre date de naissance est supérieure à une certaine date (par exemple, «j'ai plus de 18 ans») ou que vous avez plus d'un certain montant dans un compte bancaire, sans révéler le montant exact du compte ou la date de naissance.
    1. l’identité auto-souveraine (IAS)
    2. \*la preuve à divulgation nulle de connaissance
    3. portefeuilles numériques
    4. registres distribués
    5. la divulgation sélective
15. Avec \_\_\_\_\_\_\_\_\_\_, utilisant des techniques cryptographiques avancées, le vérificateur ne reçoit que les informations dont il a besoin à partir du justificatif numérique.
    1. l’identité auto-souveraine (IAS)
    2. la preuve à divulgation nulle de connaissance
    3. les portefeuilles numériques
    4. les registres distribués
    5. \*la divulgation sélective

# 

# Module 3 : Risque, protection de la vie privée et obstacles à l'adoption

## Introduction

Après avoir défini un grand nombre des termes que l'on peut rencontrer lorsqu'on explore les justificatifs numériques, nous nous intéressons maintenant à certains des autres facteurs à prendre en compte lors de l'examen d'un système ou d'un processus dépendant de justificatifs numériques. Dans ce module d'apprentissage, nous aborderons certaines des considérations importantes telles que le risque, les exigences en matière de protection de la vie privée et d'autres obstacles à l'adoption de services basés sur des justificatifs numériques.

**Objectifs d'apprentissage**

1. Définir le risque, la confiance et les niveaux de préjudice
2. Définir les niveaux d'assurance (NdA)
3. Examiner l'atténuation des risques
4. Analyse de la protection de la vie privée
5. Examiner les facteurs influençant l'adoption des justificatifs numériques

## Risque et niveau d'assurance (NdA)

### Qu'est-ce que le risque et le NdA?

Plus tôt, nous avons évoqué des concepts tels que les degrés de confiance et les niveaux d'assurance en définissant la terminologie relative aux justificatifs numériques. L'utilisation d'un justificatif numérique établit un niveau de confiance entre les entités, leur permettant d'avoir un certain degré de confiance dans la transaction à venir.

Comment tous ces concepts sont-ils liés entre eux? Comment sont-ils classés et gérés? Quel effet cela a-t-il sur l'identité numérique et les justificatifs vérifiables?

Tout au long de ce programme d'apprentissage, nous faisons référence aux niveaux d'assurance. Partons de là. Il convient tout d'abord d'éliminer certaines définitions. Nous parlons de « risque », de « niveaux d'assurance », de « confiance » et de « niveaux de préjudice ». Pour nous assurer que nous sommes sur la même longueur d'onde en explorant ces concepts, le **risque** est la *probabilité* d'un préjudice en cas d'exposition à une menace précise. Nous avons utilisé les niveaux d'assurance et les niveaux de confiance de manière quelque peu interchangeable, car ils sont très étroitement liés. L'Organisation internationale de normalisation ([ISO/IEC 29115](https://www.iso.org/fr/standard/45138.html)) définit un **niveau d'assurance** comme *décrivant le degré de confiance dans les processus menant à l'authentification et l'incluant (traduit de l’anglais).*

### Cadres des NdA

Au Canada et ailleurs dans le monde, les politiques et les standards classent souvent les niveaux d'assurance (NdA) dans un cadre défini directement associé au niveau potentiel de préjudice résultant d'une transaction compromise. En d'autres termes, le niveau d'assurance le plus bas implique une faible confiance dans les assertions et à l'attente d'un préjudice minimal ou nul dans le cas d’une transaction compromise. Au Canada, la plupart des définitions du NdA sont basées sur les [définitions officielles du NdA utilisées par le gouvernement fédéral](https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=30678&section=html).

[Can use the graphic on LoA here - see Slide 7](https://docs.google.com/presentation/d/1M1405CpKI1wqggJObbdJMJajnGSdEAwK76wgU3MEsZ8/edit#slide=id.gc78cff3fbc_0_19)

Ce sont :

* NdA 1 - Peu de confiance est requise quant au fait qu'un individu est bien celui qu’il prétend être. On peut raisonnablement s'attendre à ce que la compromission cause un préjudice nul ou minime.
* NdA 2 - Il faut avoir une certaine assurance qu'un individu est bien celui qu’il prétend être. On peut raisonnablement s'attendre à ce que la compromission cause un préjudice minimal à modéré.
* NdA 3 - Niveau d'assurance élevé qu'un individu est bien celui qu’il prétend être. On peut raisonnablement s'attendre à ce que la compromission cause un préjudice modéré à grave.
* NdA 4 - Niveau d'assurance très élevé qu'un individu est bien celui qu’il prétend être. On peut raisonnablement s'attendre à ce que la compromission cause un préjudice grave à catastrophique.

Cette classification des NdA fournit un cadre important pour la gestion et l'utilisation de justificatifs numériques. Par exemple :

* Si la **validation** et la **vérification** de justificatifs numériques sont requises à un certain niveau pour toute **authentification**, le niveau de rigueur appliqué à l'examen des justificatifs numériques diffère selon le NdA. Une identité autodéclarée peut être jugée appropriée comme base d'une **authentification** destinée à être utilisée dans une transaction de NdA 1, tandis qu'une transaction de NdA 3 peut exiger une **identité vérifiée** et des **justificatifs d'identité vérifiables** pour l'authentification.
* Les objectifs des politiques peuvent être exprimés en termes de NdA. Par exemple : « Pour les transactions de NdA 1, nous établirons un justificatif numérique sur la base de preuves contextuelles, mais pour les transactions de NdA 2, le justificatif délivré doit être basé sur au moins une preuve d'identité fondamentale ».
* Les différences de procédures peuvent être exprimées en termes de NdA. Par exemple : « pour les transactions de NdA 1, nous utiliserons les meilleures pratiques en matière de mots de passe et nous authentifierons sur cette base, mais pour les transactions de NdA 2, l'authentification doit être basée sur au moins deux facteurs ou **authentifiants** ».
* Les organismes de standardisation peuvent définir des critères de conformité pour la certification de conformité avec des niveaux croissants de rigueur et de vérification diligente en fonction du NdA.

### Exemple d’atténuation des risques

Prenons un exemple plus explicite pour aider à comprendre comment des définitions et des standards communs peuvent contribuer à faciliter les transactions en ligne.

Steve vit à Calgary et travaille à l'obtention de son diplôme d'ingénieur. Jusqu'à présent, il a pu payer ses études grâce à ses économies et aux revenus de ses emplois à temps partiel. Cependant, les exigences de l'université augmentant, Steve se rend compte qu'il aura besoin de prêts étudiants pour financer ses études.

Comme Steve utilise autant que possible les services en ligne pour faciliter sa vie occupée, il s'est déjà inscrit pour obtenir une identité numérique *MyAlberta* (MADI). Il a également suivi le processus pour s'assurer que son identité numérique *MyAlberta* était **vérifiée** (en permettant à la province d'accéder à ses renseignements sur le registre des conducteurs) afin qu'il puisse avoir accès à davantage de services en ligne qui exigent un niveau plus élevé d'assurance de l'identité.

Steve se rend sur le site internet de l'*Alberta Student Aid*, où il voit qu'il peut faire une demande en ligne après avoir créé un compte. Pour ce faire, il peut demander la création d'une nouvelle identité numérique et d’un nouveau justificatif auprès de l'*Alberta Student Aid*, ou simplement utiliser son identité numérique *MyAlberta* (MADI) existant. Il se connecte et commence sa demande de prêt étudiant. Le programme MADI a élaboré des **politiques** et des **procédures** qui s'alignent sur les **standards** établis pour un niveau d'assurance plus élevé. Celles-ci ont été examinées et déclarées conformes. Cela permet à des organismes tels que l'*Alberta Student Aid* de tirer parti du justificatif MADI et de ses assertions relatives à la validité et à la véracité, pour offrir un meilleur service aux utilisateurs de manière plus efficace.

La dépendance croissante envers l'économie numérique et la valeur toujours plus grande des transactions effectuées en ligne signifient que l'exposition au risque et le potentiel de préjudice continueront d'augmenter à mesure que l'économie numérique évoluera. Les cadres fondés sur le risque qui servent de base à des définitions communes et à des processus compris par tous sont essentiels pour fournir au moins l'un des principaux fondements d'une utilisation cohésive, sûre et respectueuse de la vie privée des justificatifs numériques.

### Rencontrer Mike

Suivons Mike pendant qu'il s'inscrit et utilise son justificatif numérique pour des services bancaires en ligne.

Nous verrons certaines des mesures utilisées pour favoriser la confiance que les consommateurs doivent avoir lorsqu'ils utilisent leurs justificatifs numériques. Cet exemple montre également l'utilisation d'approches plus strictes en matière d'authentification pour les transactions de plus grande valeur et nécessitant une plus grande confiance dans leur authenticité (c'est-à-dire le niveau d'assurance requis).

## Protection de la vie privée

### Concepts et législation sur la protection de la vie privée

**La *Loi sur la protection des renseignements personnels* et la LPRPDE**

Lorsqu’on y pense, les informations contenues dans un justificatif numérique, lorsqu'elles sont associées à la transaction dans laquelle le justificatif a été utilisé, sont généralement constituées de renseignements personnels. Dans certains cas, les justificatifs numériques peuvent même contenir des renseignements personnels sans un contexte de transaction. Pour protéger ces renseignements personnels, le Canada dispose de deux importantes lois fédérales sur la protection de la vie privée, soit la [*Loi sur la protection des renseignements personnels*](https://laws-lois.justice.gc.ca/fra/lois/p-21/index.html) et la *Loi sur la protection des renseignements personnels et les documents électroniques* ([LPRPDE](https://laws-lois.justice.gc.ca/fra/lois/p-8.6/index.html)).

* **La *Loi sur la protection des renseignements personnels* porte sur la façon dont le gouvernement fédéral doit traiter les renseignements personnels, et sur les droits d'une personne à accéder à ses renseignements personnels et à les corriger.**
  + Les gouvernements provinciaux ont également leurs propres lois régissant la protection de la vie privée dans leur domaine de compétence.
* La LPRPDE établit les obligations légales des organisations du secteur privé engagées dans des activités à but lucratif.

**La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)**

La LPRPDE s'applique aux organisations du secteur privé qui exercent leurs activités dans toutes les provinces et tous les territoires, sauf au Québec, en Alberta et en Colombie-Britannique. Ces trois provinces ont adopté leurs propres lois sur la protection de la vie privée (pour les organisations sous réglementation provinciale), que le gouvernement fédéral a examinées et jugées équivalentes à la LPRPDE.

En plus de ces lois d'application générale, plusieurs provinces ont adopté des lois sur la protection de la vie privée propres au secteur de la santé. Dans tous les cas, les éléments de protection des données personnelles de ces lois ont également été examinés et jugés équivalents à la LPRPDE. Les provinces qui ont mis en œuvre des lois dans ce domaine sont la Nouvelle-Écosse, Terre-Neuve-et-Labrador, le Nouveau-Brunswick et l'Ontario.

Le cadre juridique canadien continue d'évoluer avec le projet de [loi sur la mise en œuvre de la Charte numérique](https://www.ic.gc.ca/eic/site/062.nsf/fra/h_00108.html) qui créera la *Loi sur la protection de la vie privée des consommateurs*. Cette loi, ainsi qu'une loi «sœur» (la *Loi sur le Tribunal de la protection des renseignements personnels et des données*) créant un tribunal d'application, remplacerait et étendrait des éléments de la LPRPDE pour former l'une des lois les plus complètes en matière de protection de la vie privée. Par ailleurs, le gouvernement fédéral travaille également à la [modernisation](https://www.justice.gc.ca/fra/sjc-csj/lprp-pa/modern.html) de la *Loi sur la protection des renseignements personnels* qui régit le traitement des renseignements personnels.

Qu'est-ce que la vie privée? Qu'est-ce qui est privé? Commençons par définir la portée de ce à quoi nous faisons référence lorsque nous parlons de vie privée. La vie privée concerne les renseignements personnels et les droits des individus (ou des **personnes**) à la protection de ces renseignements. La LPRPDE définit les renseignements personnels *comme des informations concernant un individu identifiable.* La LPRPDE énonce [10 principes relatifs à l’équité dans le traitement de l’information](https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/p_principle/). Ces principes constituent les balises de la plupart des éléments liés à la vie privée des standards relatifs aux justificatifs numériques et à la protection des renseignements personnels.

En bref, ces principes sont:

* **Responsabilité** – une organisation doit nommer une personne responsable de la conformité aux 10 principes;
* **Détermination des fins de la collecte des renseignements** – le but de la collecte des renseignements personnels doit être divulgué;
* **Consentement** – une personne doit avoir connaissance de la collecte de renseignements personnels et y consentir;
* **Limitation de la collecte** – seuls les renseignements personnels requis peuvent être recueillis;
* **Limitation de l’utilisation, de la communication et de la conservation** – les renseignements personnels ne peuvent être utilisés ou communiqués qu'aux fins pour lesquelles ils ont été recueillis, et ne sont conservés qu'aussi longtemps que nécessaire;
* **Exactitude** – les renseignements personnels doivent être aussi exacts et actuels que possible pour répondre aux besoins en vertu desquels ils ont été recueillis;
* **Mesures de sécurité** – les renseignements personnels doivent être protégés d'une manière qui correspond à leur degré de sensibilité;
* **Transparence** – les politiques et pratiques en matière de gestion des renseignements personnels doivent être accessibles au public;
* **Accès aux renseignements personnels** – une personne doit être informée de la nature des informations recueillies et de la manière dont elles ont été utilisées, si et quand elle le demande. Elle a également le droit de faire modifier les informations incorrectes;
* **Possibilité de porter plainte à l’égard du non-respect des principes** – les personnes ont le droit de contester la conformité d'une organisation à l'un de ces principes.

Ces principes, énoncés dans la législation/la réglementation/les standards/les procédures, dictent qu'une personne doit :

* savoir ce qui est demandé et pourquoi;
* être invitée à consentir à la transmission et au partage de renseignements personnels;
* savoir comment les renseignements personnels sont utilisés et partagés;
* être assurée de la protection des renseignements personnels; et
* avoir l'assurance que seuls les renseignements nécessaires sont demandés et partagés.

Ces mesures de protection s'appliquent à tous les renseignements personnels, et pas seulement aux **attributs** d'un **justificatif d’identité** qui peuvent être des renseignements personnels. C'est important pour les organisations qui traitent des renseignements personnels. Les protections s'appliquent à toutes les transactions qui traitent des renseignements personnels.

### Protection de la vie privée dès la conception (Privacy by Design)

La protection de la vie privée dès la conception est particulièrement intéressante dans la mesure où elle fournit une approche complète et de haut niveau pour s’assurer que la vie privée est la première considération dans la conception de tout système. Développée et publiée au début des années 2000, elle a depuis été adoptée par de nombreux pays dans leurs politiques de protection de la vie privée et des renseignements personnels.

La protection de la vie privée dès la conception présente [7 principes fondamentaux](https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf) qui définissent une approche globale pour intégrer les préoccupations en matière de protection de la vie privée dans le développement des systèmes. Ces principes sont les suivants:

* **La protection de la vie privée est proactive, et non réactive -** les menaces à la vie privée devraient être anticipées et prévenues *avant* qu'elles ne se produisent.
* **La protection de la vie privée comme paramètre par défaut -** les renseignements personnels sont automatiquement protégés par défaut. Si une personne ne fait rien, sa vie privée reste intacte.
* **La protection de la vie privée intégrée à la conception -**  les préoccupations en matière de protection de la vie privée doivent être une composante essentielle de la fonctionnalité créée, et non un ajout.
* **La protection de la vie privée sans compromis -** les objectifs du système en matière de protection, ou non, de la vie privée peuvent généralement être atteints sans faire de compromis, de sorte que toutes les préoccupations sont prises en compte.
* **La protection du cycle de vie complet -** les mesures de protection de la vie privée s'appliquent tout au long du cycle de vie des informations, depuis leur création ou leur collecte jusqu'à leur destruction sécurisée.
* **L'ouverture -** toutes les pratiques commerciales et les technologies impliquées fonctionnent conformément aux *objectifs fixés* et sont soumises à une *vérification indépendante*.
* **Le respect de la vie privée des utilisateurs -** une approche centrée sur l'utilisateur qui garde les intérêts de l'individu au premier plan lors de la conception d'un système ou d'un processus.

### Rencontrez Amanda

Prenons un exemple des 10 *principes relatifs à l'équité dans le traitement de l'information* en action. Nous suivrons la société ACME dans sa démarche de création d'une offre de produits en ligne qui repose sur des justificatifs numériques.

Amanda Explainer video goes here

## Facteurs qui influencent l'adoption des justificatifs numériques

### Les cinq facteurs clés

Quels autres facteurs influencent l'adoption des justificatifs numériques? Quelles sont les préoccupations des utilisateurs finaux et comment y répondre?

Nous allons maintenant passer à l'identification de certaines des autres caractéristiques essentielles qui affectent leur adoption, en adoptant une approche centrée sur l'utilisateur. Ces caractéristiques sont les suivantes :

* **Fiabilité** - une caractéristique essentielle qui a un effet direct sur la confiance que les utilisateurs accorderont à un écosystème qui dépend des justificatifs numériques. La fiabilité éprouvée du justificatif numérique lui-même, et des processus qui l'utilisent, favorise la confiance requise par tous les participants (personnes et organisations) qui souhaitent utiliser le justificatif numérique. Parmi les sujets de préoccupation courants, citons :
  + Service fiable - le service fonctionne-t-il de manière constante et sans erreurs?
  + Processus fiable - les processus opérationnels sont-ils conformes au NdA attendu et à l'intégrité globale du système?
  + Conception fiable du service - la conception du service représente-t-elle les meilleures pratiques de conception et répond-elle entièrement aux préoccupations relatives à la protection de la vie privée?
* **Responsabilité** - les mécanismes qui prouvent certains éléments de fiabilité sont un concept clé ici. De même, les standards et les lois que nous avons mentionnés comportent tous des exigences visant à assurer la traçabilité de toutes les activités liées à l'utilisation des justificatifs numériques. Une responsabilité éprouvée est un autre élément clé pour favoriser la confiance nécessaire à l'adoption à grande échelle des justificatifs numériques. Une responsabilité démontrée fournit une base pour une confiance continue dans le service offert. La responsabilité comporte de nombreux éléments, notamment :
* la responsabilité reconnue d'une politique et d'une procédure bien communiquées. *Qui est responsable? À qui dois-je m'adresser si je rencontre un problème? Quels sont les mécanismes permettant de contester la politique ou la procédure?*
* une personne responsable de la gestion des préoccupations et des questions relatives à la protection de la vie privée est nécessaire.
* d'un point de vue opérationnel, les composants de la fiabilité doivent pouvoir être démontrés.
* **Interopérabilité** - L'interopérabilité entre les entités est la clé d'un écosystème sain, qui fonctionne correctement et qui est convivial. Prenons l'exemple d'un justificatif numérique délivré par un émetteur de confiance, reçu et sauvegardé dans un portefeuille numérique, puis soumis à un vérificateur tiers. Dans cet exemple, le justificatif numérique doit être interopérable avec le portefeuille numérique ET le processus de vérification. Sans interopérabilité, l'identité décentralisée ne peut pas fonctionner correctement et des cloisons d’identité numérique sont créées, c'est pourquoi nous qualifions l'interopérabilité d'exigence absolue. Dans le monde des justificatifs numériques, cette interopérabilité est réalisée sur la base de plusieurs composants clés:
* D'un point de vue technologique, il existe de nombreuses organisations qui développent des standards et des technologies pour répondre à divers aspects de l'interopérabilité technologique. Ces travaux sont de plus en plus importants et continuent d'évoluer.
* Exigences procédurales communes dictées par la loi ou la réglementation.
* Des standards élaborés en collaboration qui fournissent des orientations sur les meilleures pratiques en matière de processus et de technologies interopérables.
* Les politiques élaborées sur un territoire (p. ex., le Canada, la province de la Colombie-Britannique) ou dans un secteur (p. ex., la santé, les services financiers) permettent l'harmonisation et l'interopérabilité au niveau des politiques.
* **Convivialité** - partiellement liée à l'interopérabilité, la convivialité (ou la facilité d'utilisation), est une préoccupation majeure des utilisateurs finaux de tout processus dépendant de la technologie. Cela commence par la conception des interfaces utilisateur selon les meilleures pratiques, afin de s'assurer que:
  + les informations et les processus sont organisés de manière à rendre l'utilisation aussi simple que possible;
  + les interfaces utilisateur ne comportent pas d'erreurs et semblent crédibles; et
  + l'interface utilisateur s’adapte à de nombreux types de dispositifs (par exemple, écran de bureau traditionnel ET appareils mobiles).

Il existe de nombreuses sources de lignes directrices sur les meilleures pratiques visant une bonne conception de l'expérience utilisateur. La convivialité est un domaine de pratique à part entière, souvent appelé «expérience utilisateur», ou «EU» en abrégé. Si vous participez à un projet visant à offrir ou à modifier une expérience utilisateur en ligne impliquant des justificatifs numériques, vous devriez faire appel à une ressource professionnelle en matière d'EU pour vous assurer de maximiser la convivialité.

Au-delà d'une conception visuelle et d'une conception de processus efficaces, il y a d’autres considérations dont il faut aussi tenir compte et qui s’appliquent en particulier à l'utilisation des justificatifs numériques. Les processus qui dépendent des justificatifs numériques sont souvent assez sensibles aux questions de protection de la vie privée et de sécurité, et peuvent avoir un public cible homogène qui présente une caractéristique déterminante (par exemple, tous les utilisateurs potentiels sont susceptibles de travailler dans un cadre professionnel). De telles contraintes, ou toute exigence en matière de dispositif ou de connectivité, doivent être prises en compte lors de l'évaluation de la convivialité.

* **Accessibilité** - l'adoption généralisée des justificatifs numériques, ou de tout processus dépendant de la technologie, nécessite une approche où «personne n'est laissé pour compte» qui tient compte des besoins des utilisateurs potentiels qui peuvent rencontrer des obstacles à l'utilisation des outils les plus courants pour accéder à des services en ligne. Un pourcentage important du public est constitué de personnes ayant des limitations, comme les personnes à mobilité réduite ou les personnes souffrant de problèmes sensoriels (par exemple, une mauvaise vue). Il existe un grand nombre de défis qui peuvent rendre difficile ou impossible l'utilisation de dispositifs traditionnels par les personnes présentant des limitations (par exemple, un écran d'ordinateur ou un téléphone intelligent) généralement utilisés pour accéder à un service en ligne. Tout service dépendant des justificatifs numériques doit tenir compte de tout utilisateur potentiel dans la conception des interfaces pour les utilisateurs finaux. Outre les besoins des personnes ayant des limitations, les caractéristiques suivantes des utilisateurs devraient également être prises en compte lors de l'évaluation de l'accessibilité.
  + Les personnes qui ont des difficultés avec le processus
  + Les personnes qui ont des difficultés avec la technologie

### Rencontrez John

Mettons cela en pratique en examinant le processus de réflexion de John, gestionnaire du portail en ligne d'ACME inc., lorsqu'il étudie les causes potentielles de la faible adoption par les utilisateurs de leur site internet dépendant des justificatifs numériques.

John Explainer video goes here

### Vérifiez votre compréhension

Prenons un instant pour nous assurer que vous avez bien saisi les concepts que nous avons abordés jusqu'à présent. Dans cette activité, choisissez la meilleure réponse. Cette activité n'est pas chronométrée, alors n'hésitez pas à prendre votre temps pour la réaliser.

1. Le risque est la probabilité d'un préjudice en cas d'exposition à une menace précise.
   1. \*Vrai
   2. Faux
2. Au Canada, la plupart des définitions des NdA sont basées sur les définitions officielles des NdA utilisées par l’administration municipale.
   1. Vrai
   2. \*Faux
3. Les niveaux d'assurance (NdA) décrivent le degré de confiance dans le processus menant à l'authentification, y compris celle-ci.
   1. \*Vrai
   2. Faux
4. Combien de niveaux d'assurance y a-t-il?
   1. Un
   2. Deux
   3. Trois
   4. \*Quatre
5. Si la validation et la vérification de justificatifs numériques sont requises à un certain niveau pour toute authentification, le niveau de rigueur appliqué à l'examen des justificatifs numériques diffère selon le NdA.
   1. \*Vrai
   2. Faux
6. \_\_\_\_\_\_\_\_\_ porte/portent sur la façon dont le gouvernement fédéral doit traiter les renseignements personnels, et sur les droits d'une personne à accéder à ses renseignements personnels et à les corriger.
   1. La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)
   2. La *Loi sur la mise en œuvre de la Charte numérique*
   3. \*La *Loi sur la protection des renseignements personnels*
   4. Les 10 principes relatifs à l'équité dans le traitement de l'information
7. \_\_\_\_\_\_ établit/établissent les obligations légales des organisations du secteur privé engagées dans des activités à but lucratif.
   1. \*La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)
   2. La *Loi sur la mise en œuvre de la Charte numérique*
   3. La *Loi sur la protection des renseignements personnels*
   4. Les 10 principes relatifs à l'équité dans le traitement de l'information
8. La protection de la vie privée dès la conception présente \_\_\_\_ principes fondamentaux qui définissent une approche globale pour intégrer les préoccupations en matière de protection de la vie privée dans le développement des systèmes.
   1. 5
   2. 6
   3. \*7
   4. 8
9. Les facteurs clés qui influencent l'adoption des justificatifs numériques, en adoptant une approche centrée sur l'utilisateur, comprennent tous les facteurs suivants sauf lequel?
   1. Interopérabilité
   2. Fiabilité
   3. Convivialité
   4. Accessibilité
   5. Responsabilité
   6. \*Protection de la vie privée
10. Les renseignements personnels sont définis comme des informations concernant une personne identifiable.
    1. \*Vrai
    2. Faux

## Entrevues avec des experts

### Entrevue avec Catherine Desgagnes-Belzil

Nous avons eu l'occasion de nous entretenir avec Catherine Desgagnés-Belzil, vice-présidente exécutive et responsable de la performance d’affaires et des technologies de l'information chez Beneva. Catherine apporte une perspective unique issue de sa grande expérience avec les justificatifs numériques dans les secteurs public et privé. Catherine a partagé avec nous certaines des considérations importantes affectant l'interopérabilité, et certaines des clés pour atteindre une interopérabilité sans faille dans un écosystème.

[Insert Catherine interview here]

### Entrevue avec Dr. Ann Cavoukian

Nous avons eu le privilège de réaliser une entrevue avec Anne Cavoukian, qui a dirigé le développement initial de la protection de la vie privée dès la conception et continue de plaider pour son adoption.

Insert Ann C interview here

### Entrevue avec Michelle Chibba

Nous sommes heureux de pouvoir présenter une entrevue avec Michelle Chibba, travaillant autrefois au Commissariat à la protection de la vie privée de l'Ontario, et actuellement conférencière de renom sur la protection de la vie privée et le vol d'identité. Mme Chibba soulignera certaines des principales préoccupations liées au vol d'identité et certains des défis qui nous attendent.

[M. Chibba interview to be inserted here]

## Conclusion

Ce module a déterminé certains des facteurs importants à prendre en considération lors de la création d'un système dépendant des justificatifs numériques. La protection de la vie privée, les niveaux d'assurance, la convivialité, la fiabilité et d'autres facteurs influençant l'adoption par les utilisateurs finaux sont des facteurs déterminants dans l'adoption des justificatifs numériques.

Dans les modules d'apprentissage à venir, nous relierons tous les concepts explorés à ce jour pour décrire l'écosystème plus large dans lequel les justificatifs numériques existent et certaines des technologies et certains des standards importants utilisés pour créer et gérer les justificatifs numériques.

## Questionnaire du module 3

Vous n'avez qu'un seul essai pour répondre à ce questionnaire sur le module comportant vingt (20) questions. Ce questionnaire n'est pas chronométré, alors prenez votre temps pour examiner attentivement les choix de réponses.

1. La/L’\_\_\_\_\_\_\_\_\_\_ ne fait pas partie des 10 principes relatifs à l'équité dans le traitement de l'information contenus dans la LPRPDE.
   1. Limitation de la collecte
   2. Responsabilité
   3. Fiabilité\*
   4. Exactitude
2. «Les menaces à la vie privée devraient être anticipées et prévenues avant qu'elles ne se produisent» fait partie de la/des \_\_\_\_\_\_\_\_\_\_.
   1. LPRPDE
   2. 10 principes relatifs à l'équité dans le traitement de l'information
   3. \*protection de la vie privée dès la conception
   4. Loi sur la protection des renseignements personnels
3. Les principes de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), inscrits dans la législation/la réglementation/les standards/les procédures, dictent tous les éléments suivants SAUF :

Une personne devrait:

* 1. savoir ce que l'on demande et pourquoi;
  2. être invitée à consentir à la communication et au partage de renseignements personnels;
  3. avoir la possibilité de modifier ses propres informations privées à tout moment;
  4. \*savoir comment les renseignements personnels sont utilisés et partagés;
  5. être assurés de la protection des renseignements personnels; et,
  6. avoir l'assurance que seules les informations nécessaires sont demandées et partagées.

1. La vie privée concerne les renseignements personnels et le droit des individus (ou des personnes) à la protection de ces renseignements.
   1. \*Vrai
   2. Faux
2. \_\_\_\_\_\_\_\_\_\_\_ fournit une base pour une confiance continue dans le service offert.
   1. La protection de la vie privée
   2. La convivialité
   3. L’interopérabilité
   4. \*La responsabilité
3. Si vous participez à un projet visant à offrir ou à modifier une expérience utilisateur en ligne impliquant des justificatifs numériques, vous devriez faire appel à une ressource professionnelle en matière d'EU pour vous assurer de maximiser \_\_\_\_\_\_\_\_\_\_.
   1. la fiabilité
   2. \*la convivialité
   3. l’accessibilité
   4. l’interopérabilité
4. Il y a \_\_\_ facteurs clés qui influencent l'adoption des justificatifs numériques.
   1. 3
   2. \*5
   3. 7
   4. 10
5. Il existe trois grands composants de la fiabilité. Lequel des éléments suivants n'en fait pas partie?
   1. \*Preuve de fiabilité
   2. Service fiable
   3. Processus fiable
   4. Conception fiable du service
6. La responsabilité comporte de nombreux éléments, notamment
   1. une responsabilité reconnue pour une politique et une procédure bien communiquées.
   2. une personne responsable de la gestion des préoccupations et des questions relatives à la protection de la vie privée doit être désignée.
   3. l'audit de la procédure opérationnelle et de l'activité du système automatisé
   4. \*tout ce qui précède.
7. L'intégration harmonieuse de toutes ces parties pour fournir ce qui semble être un service unique exige en réalité un haut degré
   1. \*d'interopérabilité
   2. de fiabilité
   3. d’accessibilité
   4. de convivialité
8. La/L’ \_\_\_\_\_\_\_\_\_ éprouvée du justificatif numérique lui-même, et des processus qui l'utilisent, favorise la confiance requise par tous les participants (personnes et organisations) qui souhaitent utiliser le justificatif numérique.
   1. interopérabilité
   2. \*fiabilité
   3. accessibilité
   4. convivialité
9. L'adoption généralisée des justificatifs numériques, ou de tout processus dépendant de la technologie, nécessite une approche où «personne n'est laissé pour compte» qui tient compte des besoins des utilisateurs potentiels qui peuvent rencontrer des obstacles à l'utilisation des outils les plus courants pour accéder à des services en ligne.
   1. interopérabilité
   2. Fiabilité
   3. \*Accessibilité
   4. Convivialité
10. L'Organisation internationale de normalisation définit un niveau d'assurance comme décrivant le degré de confiance dans les processus menant à l'authentification et l'incluant.
    1. \*Vrai
    2. Faux
11. Peu de confiance est requise quant au fait qu'un individu est bien celui qu’il prétend être. On peut raisonnablement s'attendre à ce que la compromission cause un préjudice nul ou minime. Cette définition correspond au
    1. \*NdA 1
    2. NdA 2
    3. NdA 3
    4. NdA 4
12. Niveau d'assurance très élevé qu'un individu est bien celui qu’il prétend être. On peut raisonnablement s'attendre à ce que la compromission cause un préjudice grave à catastrophique. Cette définition correspond au
    1. NdA 1
    2. NdA 2
    3. NdA 3
    4. \*NdA 4
13. La dépendance croissante envers l'économie numérique et la valeur toujours plus grande des transactions effectuées en ligne signifient que l'exposition au risque et le potentiel de préjudice continueront de diminuer à mesure que l'économie numérique évoluera.
    1. Vrai
    2. \*Faux
14. Les 10 principes relatifs à l'équité dans le traitement de l'information, énoncés dans la législation/la réglementation/les standards/les procédures, dictent qu'une personne doit : savoir ce qui est demandé et pourquoi, être invitée à consentir à la transmission et au partage de renseignements personnels, savoir comment les renseignements personnels sont utilisés et partagés, être assurée de la protection des renseignements personnels, et avoir l'assurance que seuls les renseignements nécessaires sont demandés et partagés.
    1. \*Vrai
    2. Faux
15. Les 10 principes relatifs à l'équité dans le traitement de l'information ne s'appliquent qu'aux attributs d'un justificatif qui peuvent être des renseignements personnels.
    1. Vrai
    2. \*Faux
16. La LPRPDE s'applique aux organisations du secteur privé qui exercent leurs activités dans toutes les provinces et tous les territoires, à l'exception du Québec.
    1. Vrai
    2. \*Faux
17. le Canada dispose de deux importantes lois fédérales sur la protection de la vie privée, soit la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE).
    1. \*Vrai
    2. Faux

# Module 4 : Modèles d'écosystèmes et justificatifs vérifiables

## Introduction

Dans ce module d'apprentissage, nous allons explorer l'environnement dans lequel un justificatif numérique est créé et utilisé. Nous avons vu précédemment qu'un justificatif numérique est une représentation électronique d'une identité numérique. L'environnement dans lequel ce justificatif numérique est utilisé se compose de nombreux éléments tels que les participants autorisés, leurs réserves d'informations, leurs processus et les outils employés pour créer ou utiliser des justificatifs numériques. Dans le contexte de ce programme d'apprentissage, le justificatif numérique est au cœur de la «raison d'être» de l'écosystème, et nous ferons plus particulièrement référence à un écosystème d'identité numérique dans ce module.

Objectifs d'apprentissage :

1. Définir les écosystèmes dans lesquels les justificatifs numériques sont créés et utilisés
2. L'importance de la confiance
3. Modèles d'écosystèmes

## Écosystèmes d'identité numérique

### Définir l'écosystème de l'identité numérique

Plus tôt dans notre programme d'apprentissage, nous avons fait référence aux *écosystèmes* dans lesquels un justificatif numérique est créé et utilisé. Qu'entendons-nous par là? Commençons par les bases.

La définition de l'écosystème que nous avons choisi d'utiliser explique qu'il s'agit d'un:

*réseau complexe ou d'un système interconnecté* (Oxford, *traduit de l’anglais*)

ou

*de quelque chose (comme un réseau d'entreprises) considéré comme ressemblant à un écosystème écologique, notamment en raison de ses parties complexes et interdépendantes* (Merriam-Webster, *traduit de l’anglais*).

Plus loin dans ce module, nous parlerons de certaines des plus importantes activités au sein d'un écosystème (par exemple, créer des justificatifs numériques, utiliser des justificatifs numériques) et du cycle de vie d'un justificatif numérique. L'environnement global dans lequel existe un justificatif numérique est l'écosystème de l'identité numérique.

L'écosystème dans lequel un justificatif numérique est créé et utilisé repose sur une fondation composée de plusieurs éléments essentiels qui dépendent de la ou des fondations qui leur sont inférieures, comme le montre la figure ci-dessus. Un écosystème sain sera basé sur les éléments suivants:

● **Lois et règlements** - ils régissent la protection de la vie privée et des informations;

●  **Standards** - standards formels et informels qui favorisent la confiance et l'interopérabilité;

●  **Infrastructure** - les bases techniques sur lesquelles les systèmes de gestion des justificatifs numériques sont construits;

**● Créateurs de justificatifs numériques** - les organisations responsables de la création de justificatifs numériques;

●  **Gestionnaires de justificatifs numériques** - les organisations responsables de la gestion des justificatifs numériques créés; et

●  **Utilisateurs de justificatifs numériques** - les sujets de justificatifs numériques et les organisations qui dépendent de justificatifs numériques pour fournir des services.

La vidéo ci-dessous nous donne un aperçu additionnel de ces éléments essentiels d'un écosystème d'identité numérique.

<<The animated build of the pyramid goes here>>

### Considérations importantes

Avec toutes ces entités nécessaires à un écosystème dynamique et de confiance, nous pouvons voir comment certains des concepts présentés dans les modules d'apprentissage précédents sont particulièrement importants. Plus précisément, l'adoption d’un ensemble commun de standards technologiques et relatifs aux processus pouvant faire l’objet d’un audit est une exigence absolue pour assurer l'interopérabilité, la sécurité, la protection de la vie privée et la confiance nécessaires à une utilisation efficace des justificatifs numériques.

Enfin, il est important de noter qu'il n'y a pas qu'un seul écosystème. Il en existe plusieurs. Par exemple, une personne qui travaille dans un environnement sécurisé dépendant de justificatifs numériques, qui aime jouer en ligne et participer aux médias sociaux pendant son temps libre, et qui effectue la majeure partie de ses opérations bancaires en ligne, participe à au moins trois écosystèmes distincts.

Les écosystèmes peuvent choisir d'interagir les uns avec les autres. Par exemple, votre justificatif pour un média social peut également être utilisé dans une communauté de jeu en ligne. Dans ce cas, un justificatif numérique est reconnu dans plusieurs écosystèmes.

### Confiance

Dans un module d'apprentissage précédent, nous avons examiné le cadre juridique et réglementaire au Canada applicable à la protection des renseignements personnels et aux justificatifs numériques. Nous avons vu que ces lois et règlements constituent une base importante pour un écosystème sain.

Les standards qui favorisent l'interopérabilité et l'application uniforme de la sécurité et de la protection de la vie privée chez tous les participants d'un écosystème constituent un autre fondement important pour un écosystème sain. La clé de la viabilité des justificatifs numériques est la confiance. La confiance :

* qu’une personne, une organisation ou une entité est qui/ce qu'elle prétend être;
* que le processus de délivrance des justificatifs numériques est rigoureux;
* que les assertions d'identité et les autres assertions ou preuves sont valides et infalsifiables; et,
* que la vie privée est respectée.

Une confiance générale dans les justificatifs numériques favorise l'adoption par les sujets des justificatifs numériques et les organisations qui en dépendent. L'interopérabilité est rendue possible en s'assurant que les processus et les technologies employés dans la gestion des justificatifs numériques sont uniformes, cohérents et répondent au niveau d'assurance requis par tous les participants de l'écosystème. Les standards développés en collaboration sont la pierre angulaire pour atteindre les objectifs de renforcement de la confiance et de l'interopérabilité.

### 

## Standards et cadres de référence

### Qu'est-ce que le Cadre de confiance pancanadien (CCP)?

L'un des cadres de référence auxquels nous avons fait référence tout au long de ce programme d'apprentissage est le Cadre pancanadien de confianceMC (CCP).

Le CCP a été élaboré grâce à une approche collaborative entre le Conseil canadien de l’identification et de l’authentification numériques ([CCIAN](https://diacc.ca/fr/)), le Conseil des dirigeants principaux de l'information du secteur public ([CDPISP](https://citizenfirst.ca/fr/councils/public-sector-chief-information-officer-council-pscioc)) et le Conseil de la prestation des services du secteur public ([CPSSP](https://citizenfirst.ca/fr/councils/public-sector-service-delivery-council-pssdc)). Le CPSSP et le CDPISP rassemblent des responsables des standards et de la prestation de services des trois niveaux du secteur public au Canada (fédéral, provincial/territorial et municipal). Le CCIAN est une coalition à but non lucratif de dirigeants des secteurs public et privé qui se concentre sur le développement d'un cadre de référence pour l'identité et l'authentification numériques.

Qu'est-ce que le CCP? Que fait-il pour nous? Voyons cela de plus près.

Le CCP vise à renforcer la confiance des personnes et des organisations (c'est-à-dire, les utilisateurs finaux des services dépendant de l'identité numérique) dans le fait que leur identité et leurs renseignements personnels sont correctement protégés, divulgués et utilisés. Il vise à fournir une base aux gouvernements et aux entités du secteur privé qui dépendent de justificatifs numériques fiables pour fournir des services à l'aide d'un ensemble de processus standardisés de haute intégrité sur lesquels ils peuvent s’appuyer. Le CCP décrit les rôles, les services et les exigences pour assurer l'alignement, l'interopérabilité et la confiance des solutions de justificatifs numériques qui sont destinées à fonctionner au-delà des frontières organisationnelles, industrielles et juridictionnelles.

Le CCIAN établit 10 exigences pour le CCP, tout en reconnaissant que celles-ci peuvent être renforcées par des exigences supplémentaires propres à un secteur de compétence ou à un secteur industriel. Ces exigences sont les suivantes. L'écosystème de l'identité numérique doit:

● être robuste, sûr et évolutif;

● instaurer, protéger et améliorer le respect de la vie privée dès la conception;

● faire preuve de transparence dans la gouvernance et le fonctionnement;

● être inclusif et ouvert, et répondre aux besoins globaux des parties prenantes;

● offrir choix, contrôle et commodité aux Canadiens;

● tirer parti des protocoles basés sur des normes ouvertes;

● être interopérable avec les standards internationaux;

● être rentable et ouvert aux forces de la concurrence du marché;

● pouvoir faire l'objet d'une évaluation, d'un audit et d'une mise en application indépendants; et,

● minimiser le transfert de données entre les sources faisant autorité et ne pas créer de nouvelles bases de données d'identité

### Processus standardisés du CCP

Le CCP accomplit ceci en définissant les processus standardisés et les rôles des participants au sein de l'écosystème de l'identité numérique. Ceux-ci ont été décrits dans plusieurs composants du CCP, comme le montre la figure ci-dessous.

Ces composants, ainsi que les profils de conformité qui leur sont associés, peuvent être consultés sur le site internet du [CCIAN](https://diacc.ca/fr/trust-framework/), mais en bref, ils concernent les points suivants :

●  **Modèle**: décrit les buts et les objectifs du CCP.

● **Glossaire**: fournit des définitions et des exemples des termes couramment utilisés.

●  **Évaluation**: décrit le fonctionnement du programme de certification de conformité du CCP.

● **Personne vérifiée**: spécifie les processus et les critères de conformité utilisés pour établir qu'une personne physique est réelle, unique et identifiable.

● **Organisation vérifiée**: spécifie les processus et les critères de conformité utilisés pour établir qu'une organisation existe et qu'elle est réelle, unique et identifiable.

● **Justificatifs**: définit un cycle de vie des justificatifs et les critères permettant d'évaluer le degré de protection de l'utilisation des justificatifs numériques par un écosystème.

● **Authentification**: permet de s'assurer de l'intégrité constante des processus de connexion et d'authentification.

● **Avis et consentement**: définit les exigences relatives à la transmission informée, précise et complète de l'avis d'intention et du consentement pour la collecte et l'utilisation des renseignements personnels.

● **Infrastructure** : fournit les exigences générales concernant la fiabilité de l'infrastructure informatique qui soutient les processus automatisés au sein de l'écosystème de l'identité numérique.

● **Respect de la vie privée** : définit les exigences générales pour assurer l'intégrité constante des processus, des politiques et des mesures de contrôle en matière de vie privée.

La vidéo suivante nous donne un aperçu supplémentaire du contenu de chacun des profils du CCP. Veuillez noter que la vidéo n'a pas de son.

<<The animated build of the PCTF graphic goes here>>

Le CCP crée un cadre pour la confiance et l'interopérabilité de l'identité numérique au Canada. Il est également conçu pour l'évolution inévitable de l'identité numérique à mesure que nous progressons avec l'adoption de développements nouveaux et intéressants qui améliorent davantage la sécurité et la protection de la vie privée de l'identité numérique et des renseignements personnels. Le cadre est également conçu dans un souci de flexibilité et d'extensibilité. Souvent, un gouvernement ou un secteur industriel précis aura des besoins uniques. Les composants du CCP, et leurs profils de conformité, peuvent être adaptés et étendus afin de fournir un standard amélioré pour des utilisations précises.

Par exemple, le CDPISP et le CPSSP ont collaboré pour créer le [profil du secteur public du CCP](https://canada-ca.github.io/PCTF-CCP/PCTF.html) afin de répondre aux besoins uniques du secteur public canadien en matière d'identité numérique. En outre, des secteurs industriels précis ont pris en compte le CCP et son extension potentielle pour répondre aux besoins uniques de leurs écosystèmes (par exemple, la santé).

### Autres travaux notables au Canada et dans le monde

Nous avons parlé du CCP, qui se concentre sur les exigences pour favoriser la confiance nécessaire à un écosystème d'identité numérique. Deux autres organismes de standardisation canadiens méritent d'être mentionnés, car certains de leurs travaux sont directement liés à l'identité numérique et aux écosystèmes d'identité numérique. Il s'agit de :

1. Le [*Conseil canadien des normes*](https://www.scc.ca/fr) *(CCN)* est la voix du Canada au sein d'organismes de standardisation mondiaux tels que l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI). Il existe plusieurs standards dans la catégorie des technologies de l'information qui concernent les justificatifs numériques, notamment ceux publiés par le deuxième organisme de standardisation que nous souhaitons présenter.

1. Le[*Conseil Stratégique des DPI*](https://ciostrategycouncil.com/?lang=fr) *(CIOSC)* a élaboré, ou est en train d'élaborer, un certain nombre de standards liés aux justificatifs numériques.

Les standards internationaux sont nombreux. Nous vous encourageons à explorer les liens de cette section pour en savoir plus.

L'[*Organisation internationale de normalisation*](https://www.iso.org/fr/home.html) *(ISO)* comprend une myriade de standards technologiques propres aux outils qui peuvent être utilisés pour faciliter des processus tels que l'authentification (par exemple, biométrie, cartes à puce, signatures, chiffrement). Veuillez vous référer à leur section sur les *technologies de l'information* pour les rechercher. Il existe également plusieurs standards qui traitent de sujets plus larges tels que la gestion de l'identité, la protection de la vie privée, la vérification de l'identité et l'authentification. Les normes ISO/IEC 24760-xx, 29115, 29146, 29003, 29100 et 29001 sont des exemples dans ce domaine.

Le [*World Wide Web Consortium*](https://www.w3.org/) *(W3C)* élabore des standards techniques pour le Web depuis que les standards du Web existent. Certains d'entre eux seront abordés plus en détail dans un module d'apprentissage ultérieur. Deux standards sont souvent cités lors de l'étude des justificatifs vérifiables et de l'identité décentralisée: [data model for verifiable credentials](https://www.w3.org/TR/vc-data-model/) et [specification for decentralized identifiers](https://www.w3.org/TR/did-core/).

Les standards américains sont également importants en raison de la profondeur et de l'ampleur de l'interconnexion entre nos économies, tant dans le secteur public que privé. En particulier, la conformité aux standards du *National Institute of Standards and Technology (NIST)* dans la série 800 sur la cybersécurité est souvent requise pour faire des affaires avec les organismes du secteur public américain. Au sein de cette série, la [série 800-63](https://www.nist.gov/identity-access-management/nist-special-publication-800-63-digital-identity-guidelines) est spécifiquement axée sur l'identité numérique.

Un autre standard américain, souvent requis pour faire des affaires avec des entités basées aux États-Unis, est le *Federal Information Processing Standard* [FIPS 140-2](https://csrc.nist.gov/publications/detail/fips/140/2/final), ou son successeur [FIPS 140-3](https://csrc.nist.gov/publications/detail/fips/140/3/final), qui traite des exigences en matière de cryptographie pour différents niveaux de sécurité.

### Plus de travaux internationaux

Une autre autorité fréquemment citée est l'Union européenne (UE). L'UE a élaboré plusieurs standards techniques pour favoriser l'interopérabilité au sein de l'UE. En outre, toutes les entités qui souhaitent opérer au sein de l'UE doivent démontrer qu'elles sont conformes à plusieurs de leurs standards et règlements. Il est souvent fait référence au *Règlement sur l’identification électronique et les services de confiance pour les transactions électroniques* (*eIDAS)*. Les travaux actuels de l'UE et sa vision prospective sont présentés dans la stratégie de la [décennie numérique](https://digital-strategy.ec.europa.eu/en/policies/digital-compass). Des travaux sur le développement et la mise en place d’une identité auto-souveraine conforme au eIDAS sont également en cours sous l’égide du *European Self-Sovereign Identity Framework* (ESSIF). Enfin, le *Règlement général sur la protection des données* (RGPD) est une législation importante dans le domaine de la protection de la vie privée.

Les organismes internationaux de standards ouverts sont également des contributeurs essentiels au développement des standards et des cadres de référence qui aident à gouverner les écosystèmes d'identité numérique. À titre d'exemple, la [*Linux Foundation*](https://www.linuxfoundation.org/) héberge plusieurs initiatives de collaboration visant à développer des standards techniques et de processus telles que [*Hyperledger*](https://fr.hyperledger.org/)et [*Trust over IP*](http://www.trustoverip.org).

### Vérifiez votre compréhension

Prenons un instant pour nous assurer que vous avez bien saisi les concepts que nous avons abordés jusqu'à présent. Dans cette activité, choisissez la meilleure réponse. Cette activité n'est pas chronométrée, alors n'hésitez pas à prendre votre temps pour la réaliser.

\_\_\_\_\_\_\_\_\_\_\_\_ vise/visent à renforcer la confiance des personnes et des organisations (c'est-à-dire, les utilisateurs finaux des services dépendant des justificatifs numériques) dans le fait que leur identité et leurs renseignements personnels sont correctement protégés, divulgués et utilisés. En d'autres termes, un cadre de confiance pour l'identité numérique au Canada. (\*Le CCP, Les standards du W3C, eIDAS, L’ISO)

La démonstration de la conformité au règlement européen sur la protection de la vie privée, \_\_\_\_\_\_\_\_ (acronyme), est une autre exigence pour effectuer des transactions avec les États membres de l'UE, ou au sein de l'UE. (\*RGPD, eIDAS, CCP, justificatifs vérifiables)

Les deux standards souvent cités lors de l'étude des justificatifs vérifiables et de l'identité décentralisée sont le standard *data model for verifiable credentials* et le standard *specification for decentralized identifiers* publiés par le/l’ \_\_\_\_\_\_\_ (acronyme). (\*W3C, NIST, Conseil des normes, ISO)

Les composants du CCP sont les suivants : modèle, glossaire, évaluation, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, organisation vérifiée, justificatifs, authentification, avis et consentement, infrastructure et respect de la vie privée. (\*personne vérifiée, identifiants décentralisés, identité, confiance)

Les modèles d'identité numérique \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ présentent plusieurs des mêmes risques concernant les points de défaillance uniques, la renonciation au contrôle des données des utilisateurs finaux et les dangers associés aux modèles centralisés. (\*fédérée, centralisée, auto-souveraine, décentralisée)

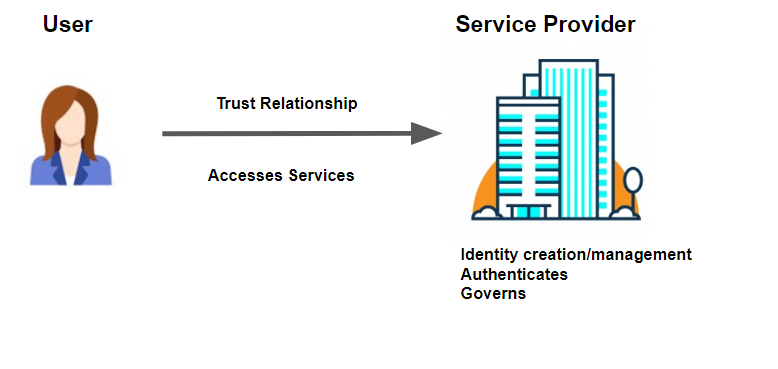
Le/L’ \_\_\_\_\_\_\_\_\_\_\_\_\_\_ est un modèle centré sur l'utilisateur, dans lequel le contrôle du partage de l'information est activement entre les mains du sujet d'une identité numérique.(\*identité décentralisée, identité centralisée, identité fédérée, CCP)

## Modèles d'écosystèmes

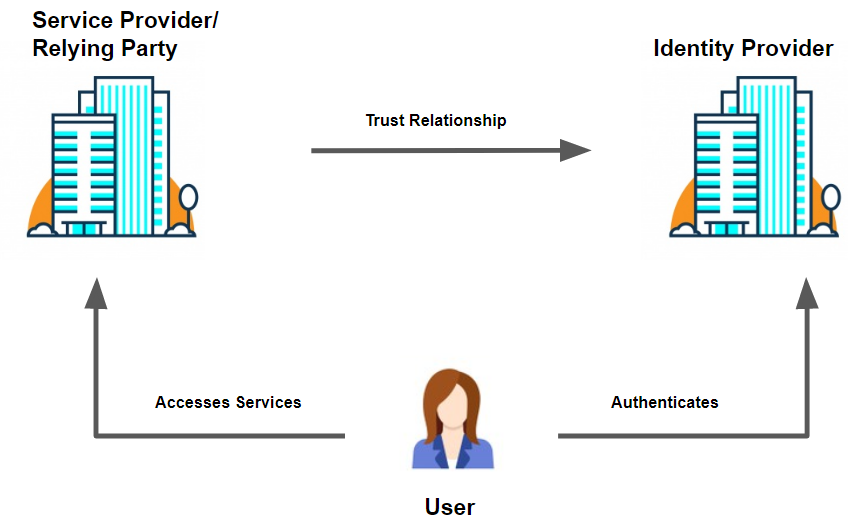
### Définir les modèles

Les écosystèmes dans lesquels les justificatifs numériques sont créés et utilisés sont mis en place à l'aide de plusieurs modèles de conception de haut niveau différents, ou de modèles d’architecture, qui peuvent servir à prédire les capacités ou le potentiel d'évolution d'un écosystème. Par exemple, la décision architecturale d'une organisation de fournir tous les services de l'écosystème avec des ressources qu'elle possède ou contrôle conduira le plus souvent à des décisions de mise en place qui lui sont propres, ce qui affecte le potentiel de croissance et de collaboration avec des organisations partenaires à mesure que l'environnement commercial évolue.

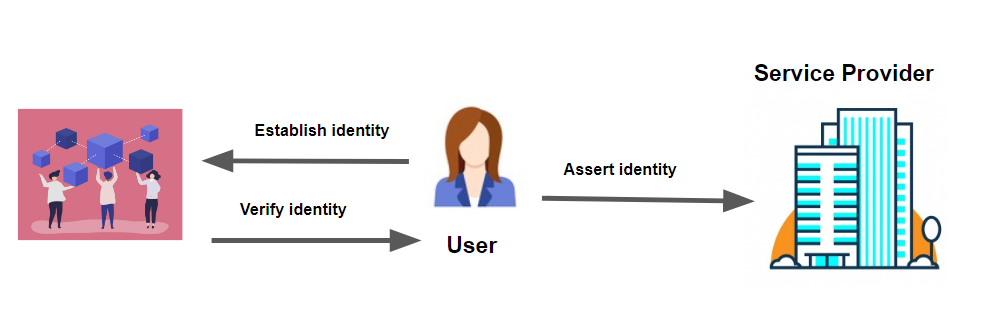
Jetons un coup d'œil à certains des modèles d'architecture courants pour un écosystème.



Centralisé - dans ce modèle, un *compte* est créé, contrôlé et détenu par l'organisation avec laquelle une personne effectue une transaction. Ce modèle est encore largement utilisé, mais n'est pas recommandé pour des raisons que nous développerons plus loin dans cette section.



Fédéré - ce modèle introduit un fournisseur d'identité. Les justificatifs établis et/ou gérés par une organisation sont utilisés pour accéder à une autre. Cela permet l'authentification unique, qui ouvre la possibilité d'utiliser un seul justificatif numérique pour accéder à plusieurs domaines.



Décentralisé - ce modèle s'appuie souvent sur la technologie de la chaîne de blocs (*blockchain*) pour utiliser des registres distribués et des techniques de cryptographie afin de créer des justificatifs numériques qui résident dans le réseau et qui sont sous le contrôle du sujet de l'identité numérique. Dans ce modèle, aucune base de données centralisée n’est nécessaire.

### Centralisé

Les modèles les plus utilisés aujourd'hui sont, de loin, les modèles centralisés et fédérés.

Les modèles centralisés étaient les plus pratiques à mettre en place dans le passé. Cependant, ils s'accompagnent de plusieurs problèmes à plus long terme, notamment :

* Par souci d'efficacité, ces systèmes n'étaient souvent pas basés sur des standards. Pour certains anciens systèmes, les standards appropriés n'existaient peut-être même pas à l'époque. L'interopérabilité et l'intégration avec d'autres systèmes, à mesure que l'utilisation des justificatifs numériques se répand, deviennent coûteuses et difficiles à maintenir;
* Les multiples points de défaillance uniques entraînent des problèmes de fiabilité;
* L'exigence d'intégrations «point à point» entre les fournisseurs de services et les vérificateurs entrave considérablement l'évolutivité à plus grande échelle (par exemple, nationale, mondiale).
* Cela conduit à la prolifération d'authentifiants pour l'utilisateur final, car chaque organisation avec laquelle il traite possède sa propre plateforme. Le risque pour l'utilisateur final augmente avec une gestion plus ardue d’éléments comme les mots de passe;
* L'utilisateur, par nécessité, renonce au contrôle de ses renseignements personnels;
* Le risque augmente également de façon exponentielle lorsqu'il existe des répertoires centralisés d'informations sur les justificatifs numériques (par exemple, une seule attaque réussie sur un répertoire compromet une quantité massive d'informations). Dans le cas du modèle centralisé, ce risque est plus élevé, car la compétence principale de l'organisation est généralement la prestation de son service commercial; et
* Les données sont souvent contenues dans des plateformes et des technologies exclusives, et la forme et les méthodes d'assertion ou d'échange de données peuvent également être exclusives. Cela réduit considérablement les possibilités d'évolution vers l'utilisation d'approches davantage basées sur des standards et la migration vers des modèles améliorés. La réinvention des systèmes s'impose plus souvent à mesure que les opérations évoluent.

### Fédéré

Les modèles d'identité fédérée présentent plusieurs des mêmes risques concernant les points de défaillance uniques, la renonciation au contrôle des données des utilisateurs finaux et les dangers associés aux répertoires centralisés. Cependant, ce modèle offre des avantages significatifs par rapport au modèle centralisé. Ces avantages sont, notamment:

* La possibilité d'accéder à plusieurs services en utilisant un seul justificatif numérique;
* Ces systèmes sont basés sur des standards avec des méthodes cohérentes pour l'échange d'informations (c'est-à-dire, les assertions); et
* Tandis que le risque d'attaque d'un répertoire centralisé d'informations existe toujours, les informations sont gérées par des organisations dont l'objectif principal est la gestion des justificatifs numériques. Le risque demeure, mais l'organisation soumise à l'attaque est généralement mieux équipée pour répondre à ces attaques.

### Décentralisé

L'identité décentralisée est un modèle centré sur l'utilisateur, dans lequel le contrôle du partage de l'information est activement entre les mains du sujet d'un justificatif numérique. Cette approche repose sur l'utilisation des approches technologiques où les informations sont sous le contrôle direct du sujet d'un justificatif numérique, et où les informations supplémentaires soutenant la vérification/validation sont hébergées sur le réseau (par exemple, les registres distribués). Le registre distribué permet de faire confiance au réseau, sans le contrôle d'une autorité centrale. Grâce au mécanisme consensuel (les ententes entre les parties sur le statut du registre), certaines informations sont répliquées, partagées et synchronisées géographiquement, dans plusieurs pays ou organisations.

Il n'existe pas d'administrateur central ou de stockage centralisé des données, puisque le réseau est formé par des pairs qui ont les mêmes droits et traitent librement entre eux. La cryptographie à clé publique permet un niveau de sécurité approprié en matière d'autorisation et de partage d'informations. Elle assure l'intégrité des données puisque les données de la transaction sont vérifiées, ainsi que la propriété des transactions elles-mêmes. Dans d'autres modules d'apprentissage, nous approfondirons ce sujet et certaines des méthodes et technologies qui ont été utilisées dans les mises en œuvre de référence du modèle décentralisé.

Ces approches décentralisées, lorsqu'elles sont mises en œuvre en utilisant les principes de l'identité auto-souveraine, promettent d'offrir plusieurs avantages que ne permettent pas les modèles traditionnels. Ces avantages sont, notamment:

* le contrôle absolu par l'utilisateur du partage des justificatifs numériques;
* des méthodes de renforcement de la protection de la vie privée qui permettent de ne partager que ce qui est absolument nécessaire;
* une meilleure protection de l'intégrité des données;
* une réduction significative de la dépendance envers des technologies particulières;
* les émetteurs de justificatifs n'ont pas besoin de faire l’intégration avec les vérificateurs;
* les émetteurs ne savent pas quand leurs justificatifs sont utilisés, ces transactions restent entre l'utilisateur et le vérificateur (meilleure protection de la vie privée);
* la vérification peut être effectuée sans utiliser la puissance de traitement de l'émetteur. Par exemple, même dans les cas où la révocation doit être vérifiée, cela peut être fait en consultant un registre distribué;
* l’élimination de la dépendance envers des autorités centralisées ou tierces pour l'authentification; et
* une réduction significative de la charge de gestion des authentifiants et des problèmes de sécurité associés à la protection des justificatifs et des authentifiants.

### Caractéristiques des écosystèmes sains

Les principaux éléments constitutifs des écosystèmes sains peuvent être caractérisés comme suit:

* Les objectifs et les principes d'un écosystème doivent être clairement définis. Cela permet d'établir une compréhension commune de la raison d'être de l'écosystème et de fixer certains des repères qui détermineront la manière dont l'écosystème est géré, voire le modèle d’implémentation.
* Ensuite, les détails qui établiront les approches opérationnelles clés pour l'écosystème. Cela inclut les décisions sur les rôles et les responsabilités des participants à l'écosystème, la manière dont l'écosystème sera gouverné et la définition des critères de base pour la participation à l'écosystème.
* Les exigences ou les critères de conformité applicables à chacun des rôles dans un écosystème sont ensuite nécessaires pour assurer une compréhension commune des responsabilités détaillées de chaque participant à l'écosystème. Cela permet également d'établir le modèle opérationnel pour la gestion des informations et de fournir une base pour l'évaluation des participants à l'écosystème.
* Avec la création de ces exigences détaillées, un programme complémentaire d'audit et de vérification de la conformité aux exigences de l'écosystème doit être établi.
* Enfin, nous voulons que l'écosystème soit flexible et capable de répondre aux évolutions des meilleures pratiques de création, de gestion et d'utilisation des justificatifs numériques. Les processus régissant l'amélioration continue de l'écosystème sont essentiels pour soutenir la viabilité à long terme d'un écosystème sain.

La liste précédente définit les éléments clés qui contribuent à un écosystème sain. Si nous partons du principe qu'il y aura un nombre varié de participants jouant des rôles uniques dans un écosystème, la *personnalité* d'un écosystème est également importante pour sa viabilité à long terme. Ce sont les principes qui définissent les attentes des personnes qui contribuent à l'évolution d'un écosystème. Parmi les caractéristiques communes des écosystèmes fonctionnels, citons :

* Ouverture - L'écosystème doit être ouvert à tout participant qualifié qui souhaite y contribuer d'une manière ou d'une autre. Il peut s'agir d'un participant opérationnel souhaitant remplir un rôle (soumis à des standards et d’autres exigences) ou d'une entité souhaitant contribuer à l'évolution de l'écosystème.
* Flexibilité - Les participants à l'écosystème doivent comprendre qu'il y aura différentes perspectives parmi les participants à l'écosystème et être prêts à accepter ces perspectives et à en tirer profit. Dans de nombreux cas, « le tout est plus grand que la somme de ses parties » : le résultat de l'apprentissage communautaire crée un écosystème plus fort.
* Extensible - La conception de l'écosystème n’empêche pas l'évolution de sa conception afin d'intégrer des approches et des technologies améliorées en matière de meilleures pratiques.
* Collaboratif - Le processus de développement et de maintenance de l'écosystème doit être consciemment inclusif, en veillant à ce que toutes les parties prenantes aient la possibilité de contribuer et que leurs perspectives et besoins uniques soient pris en considération.

### Retour sur Martin

Suivons Martin dans son expérience d'utilisation de l'identité numérique selon chacun des modèles (centralisé, fédéré et décentralisé) que nous avons définis ci-dessus.

<<Explainer video to be inserted here>>

## Entrevues avec des experts

### Entrevue avec Joni Brennan

Nous avons eu l'occasion de parler avec Joni Brennan, présidente du Conseil d'identification et d'authentification numériques du Canada (CCIAN), de ses expériences et de certaines des avancées importantes qui peuvent être réalisées dans le paysage de l'identité numérique, rendues possibles par une collaboration ouverte entre tous les principaux intervenants que nous avons mentionnés dans cette section du module d'apprentissage.

<<Joni Brennan interview goes here>>

### Entrevue avec Andrew Johnston

Andrew Johnston, vice-président du développement des standards et des relations avec l'industrie chez 2Keys, est ici pour nous donner un aperçu supplémentaire de la nature des écosystèmes d'identité numérique sains et de certains des travaux importants réalisés pour faire évoluer les écosystèmes d'identité.

<<Andrew Johnston interview goes here>>

## Conclusion

Dans ce module d'apprentissage, nous avons défini l'écosystème dans lequel un justificatif numérique peut être créé, géré et utilisé. Nous avons vu ses composants et les principaux modèles utilisés pour construire un écosystème. Nous avons également examiné certains des standards et des organismes de développement de cadres de référence des écosystèmes les plus cités au Canada et dans le monde.

Les modules d'apprentissage suivants exploreront certains des standards ouverts et des bases technologiques utilisés pour mettre en œuvre ces écosystèmes. Restez à l'affût pour en savoir plus!

## Questionnaire du module 4

Vous n'avez qu'un seul essai pour répondre à ce questionnaire de dix-sept (17) questions sur le module. Ce questionnaire n'est pas chronométré, alors prenez votre temps pour examiner attentivement les options avant de choisir la meilleure réponse.

1. Le \_\_\_\_\_\_\_\_\_\_\_ est la voix du Canada au sein d'organismes de standardisation mondiaux tels que l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI).
2. CCIAN
3. CIOSC
4. CCN\*
5. W3C
6. Dans le modèle \_\_\_\_\_\_\_\_\_, où le sujet d'un justificatif numérique traite uniquement avec le fournisseur d'un service dépendant de justificatifs numériques, l'organisation peut être le créateur/le gestionnaire/l’utilisateur d'un justificatif numérique en plus d'exploiter l'infrastructure technique dont elle dépend.
7. décentralisé
8. du fournisseur de services d'identité
9. centralisé\*
10. de l’identité numérique
11. Le modèle du CCP décrit les processus clés pour les activités comme l’authentification et la création de justificatifs numériques. Il les décrit comme appartenant à trois grandes catégories, avec les rôles suivants, SAUF :
12. Créer et gérer des identités numériques
13. Utiliser l'identité numérique
14. Empêcher l'utilisation de certaines identités numériques\*
15. Activer des systèmes d'identité numérique
16. Une personne qui travaille dans un environnement sécurisé dépendant des justificatifs numériques, qui aime jouer en ligne et participer aux médias sociaux pendant son temps libre, et qui effectue la majeure partie de ses opérations bancaires en ligne, participe à au moins \_\_\_ écosystèmes d'identité numérique distincts.
17. Un
18. Deux
19. Trois\*
20. Quatre
21. Votre identité sur un média social peut également être utilisée dans une communauté de jeu en ligne. C'est un exemple d'écosystèmes qui choisissent \_\_\_\_\_\_\_\_.
22. d’interopérer\*
23. de créer des justificatifs numériques
24. de modifier les processus
25. de hiérarchiser
26. Les écosystèmes d'identité numérique d’un ministère peuvent exister en tant que sous-ensemble identifiable d’un écosystème gouvernemental plus large, en s'appuyant sur les bases fournies par l'écosystème au niveau gouvernemental et en le complétant pour lui permettre d'effectuer des transactions et des activités au niveau du ministère. C'est un exemple d'écosystèmes qui choisissent \_\_\_\_\_\_\_\_.
27. d’interopérer
28. de créer des justificatifs numériques
29. de modifier les processus
30. de hiérarchiser\*
31. Les lois et règlements constituent une base importante pour un écosystème d'identité numérique sain.
32. Vrai\*
33. Faux
34. Un/Une \_\_\_\_\_ général(e) dans les justificatifs numériques favorise l'adoption par les sujets des justificatifs numériques et les organisations qui en dépendent.
35. interopérabilité
36. confiance\*
37. standard
38. niveau
39. Un chiffrement fort et une sécurité avancée pour protéger la réserve principale de renseignements personnels sont des caractéristiques des modèles d'écosystèmes décentralisés.
40. Vrai
41. Faux\*
42. Le CCIAN établit \_\_\_ exigences pour le CCP, tout en reconnaissant que celles-ci peuvent être renforcées par des exigences supplémentaires propres à un secteur de compétence ou à un secteur industriel.
43. 5
44. 10\*
45. 15
46. 20
47. \_\_\_\_\_ se concentre sur les exigences pour favoriser la confiance nécessaire à un écosystème d'identité numérique.
48. Le CCP\*
49. Le CCN
50. L’ISO
51. Le CIOSC
52. Les émetteurs de justificatifs numériques doivent disposer de systèmes solides pour que les justificatifs qu'ils délivrent puissent être vérifiés lors de leur utilisation.
53. Vrai
54. Faux\*
55. Le risque pour les utilisateurs finaux est généralement plus élevé lorsqu'ils participent à un écosystème \_\_\_\_\_\_\_\_\_ pour la délivrance et la gestion des justificatifs numériques.
56. Fédéré
57. Centralisé\*
58. Décentralisé
59. Réglementé
60. La démonstration de la conformité au RGPD est une exigence pour effectuer des transactions contenant des données personnelles avec des États membres de l'UE, ou au sein de l'UE.
61. Vrai\*
62. Faux
63. Les identités \_\_\_\_\_\_\_\_\_ tirent parti de deux caractéristiques principales de la chaîne de blocs : le registre distribué et la cryptographie.
64. distribuées
65. fédérées
66. décentralisées\*
67. centralisées
68. Dans ce modèle, un compte est créé, contrôlé et détenu par l'organisation avec laquelle une personne effectue une transaction. Ce modèle est encore largement utilisé, mais n'est pas recommandé.
69. Distribué
70. Fédéré
71. Décentralisé
72. Centralisée\*
73. Ce modèle introduit un fournisseur d'identité. Les justificatifs numériques établis et/ou gérés par une organisation sont utilisés pour accéder à une autre. Cela permet l'authentification unique, qui ouvre la possibilité d'utiliser un seul justificatif numérique pour accéder à plusieurs domaines.
74. Distribué
75. Fédéré\*
76. Décentralisé
77. Centralisé

# 

# Module 5: Justificatifs vérifiables

## Introduction

Maintenant que nous avons défini les concepts de base, examiné le cycle de vie d'un justificatif numérique, et vu certaines des façons dont un justificatif numérique est créé et géré, examinons les **justificatifs vérifiables**. Le [W3C](https://www.w3.org/TR/vc-data-model/) définit les justificatifs vérifiables comme [*un mécanisme permettant d'exprimer les justificatifs d'identité sur le Web d'une manière qui est cryptographiquement sécurisée, qui respecte la vie privée et qui est vérifiable de façon automatisée*](https://www.w3.org/TR/vc-data-model/) *(traduit de l’anglais)*.

Les justificatifs vérifiables constituent un standard ouvert pour les justificatifs numériques et représentent une base essentielle pour les modèles de justificatifs numériques pair à pair que nous avons mentionnés précédemment. Ce module d'apprentissage définit les justificatifs vérifiables et certains des concepts clés qui les sous-tendent avant de passer à d'autres considérations et technologies relatives à la conception d'écosystème dans les modules d'apprentissage suivants.

Objectifs d'apprentissage

* Expliquer les justificatifs vérifiables et l'identité vérifiée
* Analyser les assertions vérifiables
* Décrire les identifiants décentralisés

## Justificatifs vérifiables et identité vérifiée

### Justificatifs vérifiables

Un justificatif vérifié est simplement une assertion de justificatif présentée qui a fait l'objet d’une **validation** et d’une **vérification** réussies à l'aide de processus de confiance. En d'autres termes, la réponse à des questions telles que: *les informations présentées sont-elles exactes?* Et dans le contexte de l'identité d'une personne - *Appartiennent-elles à la personne qui revendique cette identité?*

Plus tôt, nous avons brièvement défini les justificatifs vérifiables comme [*un mécanisme permettant d'exprimer les justificatifs d'identité sur le Web d'une manière qui est cryptographiquement sécurisée, qui respecte la vie privée et qui est vérifiable de façon automatisée*](https://www.w3.org/TR/vc-data-model/) *(traduit de l’anglais)*. Les justificatifs vérifiables sont principalement pris en charge par deux standards développés par le World Wide Web Consortium (W3C). Plus précisément, le [Verifiable Credentials Data Model](https://www.w3.org/TR/vc-data-model/) définit une manière normalisée d'exprimer les justificatifs, et le standard [Decentralized Identifiers](https://w3c.github.io/did-core/) fournit certains des mécanismes utilisés pour vérifier ces justificatifs.

### Comment fonctionnent les justificatifs vérifiables?

Mettons de côté la manière dont ces identifiants sont gérés et consommés pour un instant et examinons de plus près les justificatifs vérifiables eux-mêmes.

Au niveau le plus simple[[1]](#footnote-0), les justificatifs vérifiables ne sont rien d'autre que l'équivalent électronique des justificatifs physiques que nous utilisons déjà aujourd'hui : cartes de crédit, passeports, permis de conduire et des choses comme des qualifications et des reconnaissances. Dans ces exemples, selon la méthode traditionnelle, dont plusieurs d'entre nous connaissent, un utilisateur partage des informations délivrées par un émetteur reconnu et approuvé avec un fournisseur de services, y compris des données personnelles très sensibles, puis, le fournisseur de services peut stocker toutes ou des parties de ces informations sur ses serveurs centralisés et les utiliser pour décider d’offrir à l'utilisateur un certain type de service, qui peut lui-même inclure la délivrance d'un nouveau type de justificatif..

Les justificatifs vérifiables peuvent être utilisés pour établir la confiance entre les parties en utilisant un ensemble d’assertions et de métadonnées inviolables qui prouvent de manière cryptographique l'identité du titulaire et de son émetteur. Plus important encore, en utilisant cette approche, les utilisateurs peuvent conserver leurs données et simplement partager les informations nécessaires sous la forme d'un justificatif vérifié avec une autre partie lorsqu'ils reçoivent une demande. La possibilité d'extraire les informations nécessaires et de ne présenter que ces informations à l’utilisateur final est appelée la *divulgation sélective*. Les justificatifs vérifiables présentent les avantages suivants : le justificatif fournit une preuve cryptographique que le document est authentique, que les informations n'ont pas été altérées, ainsi qu'une méthode d'authentification forte de l'émetteur sans que celui-ci ait à participer à l'échange. Il existe également un moyen de vérifier la révocation. Enfin, et c'est peut-être le plus important, il n'est pas nécessaire de prévoir une intégration «point à point» entre l'émetteur et le vérificateur.

Pour que les justificatifs vérifiables fonctionnent, ils doivent soutenir quatre acteurs différents : l’émetteur, le vérificateur, le sujet et le titulaire.

* Sujet : l'entité ou la chose au sujet de laquelle une assertion est donnée.
* Émetteur : la personne qui crée l’assertion et l'associe au sujet.
* Vérificateur : l'entité ou la personne qui vérifie l’assertion concernant un sujet donné.
* Titulaire : l'entité qui contrôle les justificatifs vérifiables. Un titulaire est généralement, mais pas toujours, le sujet des justificatifs vérifiables qu'il détient.

Par exemple, chaque fois que quelqu'un veut savoir quelque chose sur nous, nous pouvons utiliser l’assertion vérifiable pour partager une qualification, une réalisation, une qualité ou un élément d'information sur une entité ou une personne, comme un nom, un numéro d'identification gouvernemental, un fournisseur de paiement, une adresse de domicile ou un diplôme universitaire.

### Comment fonctionnent les assertions vérifiables?

Examinons de plus près le fonctionnement des assertions vérifiables. Il y a trois éléments clés pour un justificatif vérifiable. Il s'agit :

* d’un format de données commun compris par tous les participants. Il s'agit du format de données prescrit par le [Verifiable Credentials Data Model](https://www.w3.org/TR/vc-data-model/) du W3C ;
* d’une cryptographie protégeant toutes les données et les assertions échangées entre les participants; et
* de registres permettant la validation/vérification des données et de toutes assertions associées.

Nous allons examiner quelques processus clés, du moins à haut niveau, pour aider à illustrer comment un justificatif vérifiable est créé et consommé. Mais d'abord, examinons les fondements de ce qui rend un justificatif «vérifiable». Comme nous l'avons vu, l'examen des informations d'un justificatif numérique comporte deux aspects essentiels. Plus précisément, la **validation** pour s'assurer que les informations sont exactes, et la **vérification** pour s'assurer qu'elles appartiennent à l'entité qui est le sujet d’un justificatif numérique.

Nous avons également mentionné la cryptographie et les registres comme des éléments clés pour rendre une assertion «vérifiable». Cela repose sur des principes ancrés dans l'infrastructure à clé publique (ICP) qui utilise des clés publiques et privées pour le chiffrement, les signatures numériques et la révocation. Si vous n'êtes pas familier avec l'ICP, la partie sur l’introduction à la cryptographie de ce module d'apprentissage nous donne quelques exemples, et il existe de [nombreuses références de base disponibles en ligne](https://fr.wikipedia.org/wiki/Infrastructure_%C3%A0_cl%C3%A9s_publiques) pour aider à comprendre l'ICP.

L'utilisation de la cryptographie et d'une certaine forme de registres permet aux acteurs des clés (émetteur, titulaire, vérificateur) de réaliser les activités suivantes :

* Les justificatifs peuvent être délivrés et signés par l'émetteur, ce qui permet de s'assurer que le justificatif a bien été délivré par une entité à laquelle vous choisissez de faire confiance;
* Le titulaire peut authentifier l'émetteur et le vérificateur;
* Le titulaire peut prouver cryptographiquement qu'il détient un justificatif particulier, sans céder le contrôle total dudit justificatif au vérificateur;
* La cryptographie est utilisée pour s'assurer que seul le destinataire prévu d'une communication est en mesure de déchiffrer un message (entre l'émetteur et le titulaire, entre le titulaire et le vérificateur, etc.); et
* Le vérificateur d'une assertion peut s'assurer que les données proviennent d'un émetteur reconnu, que le justificatif est valide et que ces données n'ont pas été altérées. Le vérificateur peut également, s'il le souhaite, vérifier que le justificatif n'a pas été révoqué.

### Délivrance et utilisation d'un justificatif d'identité

Examinons la délivrance et l'utilisation d'un justificatif d'identité. La figure ci-dessous illustre, à très haut niveau, la délivrance et l’utilisation d'un justificatif vérifiable et d'une assertion vérifiable.

<<animated image to be inserted here - See Unit 5 image posted in Graphics folder on Drive>>

La figure ci-dessus suppose que le sujet du justificatif numérique est également le titulaire du justificatif délivré. Elle suppose également une vérification bidirectionnelle des entités impliquées dans la délivrance d'une assertion d'identité.

Ce n'est pas toujours le cas. Les systèmes peuvent disposer d’un titulaire tiers que le sujet a choisi pour détenir et protéger le justificatif délivré (*Remarque : certains exemples incluent des cas où l'on peut s'attendre à une relation de représentant, par exemple parent-enfant*). De même, si la vérification du sujet/titulaire est une exigence absolue, certaines implantations peuvent ne pas inclure la confirmation de l'identité du vérificateur.

Ce modèle part également du principe que toutes les parties et technologies utilisent un format de données commun, tel que le standard ouvert décrit dans le *Verifiable Credential Data Model* du W3C.

Enfin, l'illustration suppose un modèle d'écosystème pair à pair tel que décrit dans un module d'apprentissage précédent. Le *Verifiable Credentials Data Model* du W3C ne représente pas à lui seul l'ensemble des standards requis pour un échange de justificatifs vérifiables pair à pair. Des standards pour le processus (par exemple, *Decentralized Identifiers* du W3C) et des standards technologiques ouverts sont également nécessaires pour construire le modèle complet. Plus tard dans ce module d'apprentissage, nous examinerons les identifiants distribués. Nous explorerons certains des standards technologiques ouverts qui soutiennent les justificatifs vérifiables dans un autre module d'apprentissage.

## Constitution d'un justificatif vérifiable

### Délivrance de justificatifs vérifiables

Regardons de plus près comment sont constitués un justificatif vérifiable et une assertion vérifiable. Cela nous aidera à comprendre comment un justificatif vérifiable peut être [*un mécanisme permettant d'exprimer les justificatifs d'identité sur le Web d'une manière qui est cryptographiquement sécurisée, qui respecte la vie privée et qui est vérifiable de façon automatisée*](https://www.w3.org/TR/vc-data-model/) *(traduit de l’anglais)*.

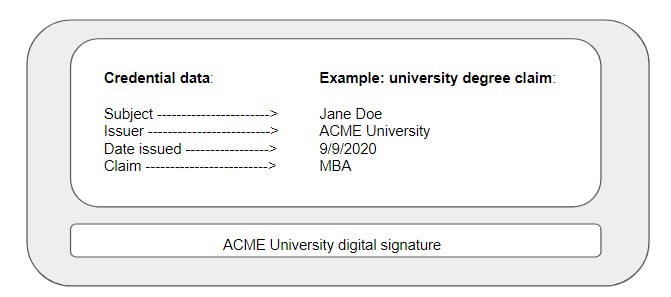
Délivrance de justificatifs vérifiables:

Un justificatif vérifiable, comme tout justificatif, fait l'objet d'une validation et d'une vérification avant d'être délivré. Une fois délivré, il se compose de deux éléments.

1. Le justificatif lui-même contient les métadonnées du justificatif, les identifiants et l’assertion (par exemple, le permis de conduire provincial de John Doe).
2. La preuve du justificatif, essentiellement l'application d'une signature numérique au justificatif délivré, assure l'immuabilité du justificatif délivré.

Une fois délivré, le justificatif est créé par l'émetteur et remis au titulaire du justificatif. La cryptographie est utilisée pour le chiffrement et la signature numérique de l'«enveloppe» contenant le justificatif afin de s’assurer que le justificatif ne peut être utilisé que par le destinataire prévu (c'est-à-dire, le titulaire) et que le titulaire peut être assuré qu'il provient de l'émetteur.

Notre exemple de justificatif vérifiable ressemble à quelque chose comme ceci :

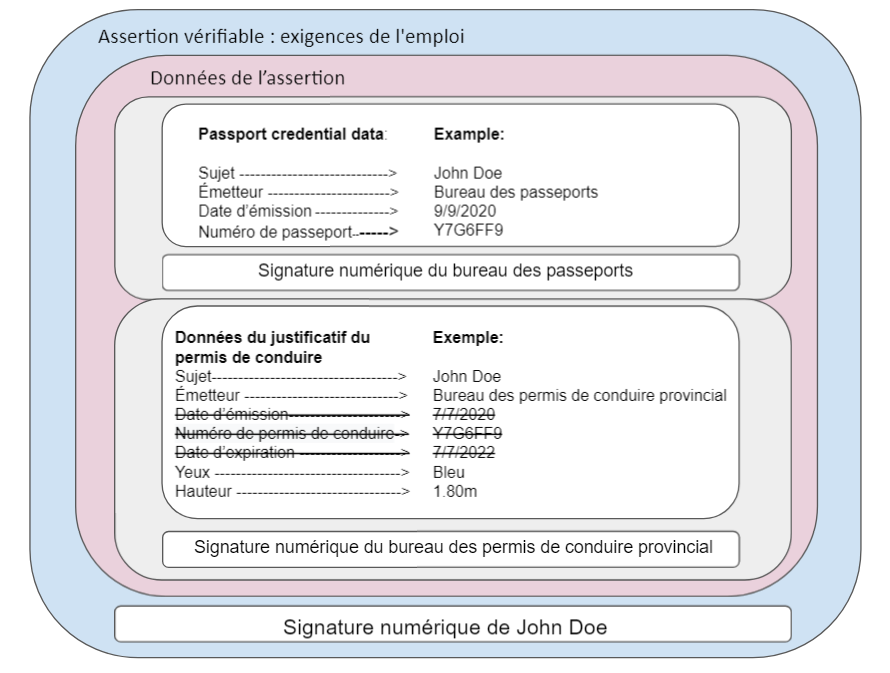


### Assertions vérifiables

Une assertion vérifiable consiste en des données d’identification extraites d'un ou plusieurs justificatifs assemblés pour être présentés dans un contexte spécifique. C'est ce que le titulaire présente au vérificateur avec lequel il souhaite établir une identité numérique dans le but de recevoir un service en ligne.

Prenons un exemple que la plupart d'entre nous peuvent comprendre.

John postule pour un emploi qui comporte deux exigences strictes : il doit être citoyen canadien et posséder un permis de conduire valide. John a reçu un justificatif vérifiable du bureau des passeports canadiens avec son justificatif de passeport. Il détient également un justificatif vérifiable du bureau des permis de conduire de sa province de résidence. De son justificatif de passeport, son nom et son numéro de passeport sont requis. De son permis de conduire, son nom, son numéro de permis et la date d'expiration sont requis. Ces informations regroupées dans une présentation uniforme des assertions affirmant les deux exigences (c'est-à-dire, être un citoyen canadien et détenir un permis de conduire valide) seront requises. À un niveau élémentaire, cette assertion vérifiable serait constituée de la manière suivante :



Tout comme un justificatif individuel, une assertion auprès d'un vérificateur est constituée de deux composants de base, les données qui composent l’assertion et la signature de l'entité qui fait l’assertion.

Il est important de noter que, dans cet exemple, ce ne sont pas toutes les données du passeport, ni celles du permis de conduire, qui ont été utilisées pour construire l'assertion vérifiable qui est faite. Par exemple, les données du justificatif du permis de conduire comprennent des attributs indiquant que John Doe a les yeux bleus et mesure 1,8 mètre. Bien que cela fasse partie du justificatif délivré, il est possible de n'inclure que les informations requises par le vérificateur. Bien entendu, cela dépendra également de la configuration de la technologie utilisée pour construire l'assertion vérifiable ou le justificatif vérifiable. Toutefois, les standards utilisés n'excluent pas ce niveau de précision dans la constitution d'une assertion d'identité (pour plus d’informations, veuillez voir l’introduction à la divulgation sélective *plus loins dans ce série d’apprentissage*).

Cela est important du point de vue de la protection de la vie privée, car au lieu de partager l'intégralité du justificatif, seuls les informations ou les attributs d'identité requis sont partagés. Le fait que le vérificateur n'ait pas le contrôle total du justificatif délivré est une autre caractéristique importante.

### Justificatifs vérifiables et assertions vérifiables en action

Regardez la vidéo ci-dessous pour un autre exemple de cette approche en action.

<<explainer video goes here - I was thinking of building an example of registering for a site that requires two pieces of ID, at least one with a picture and one Govt issued with date of birth - show how it works now and then how it would work using a digital wallet and verifiable credentials>>

Revenons à notre définition des justificatifs vérifiables et voyons si l'exemple ci-dessus répond aux critères de notre définition des justificatifs vérifiables - à savoir [*un mécanisme permettant d'exprimer les justificatifs d'identité sur le Web d'une manière qui est cryptographiquement sécurisée, qui respecte la vie privée et qui est vérifiable de façon automatisée*](https://www.w3.org/TR/vc-data-model/) *(traduit de l’anglais)*. Examinons chacune des exigences de cette définition.

* Cryptographiquement sécurisé - L’assertion ou le justificatif est signé et chiffré à l'aide des paires de clés publiques et privées des entités qui effectuent la transaction. Cela répond à trois objectifs importants : les données ne peuvent être déchiffrées que par l'entité qui en est le destinataire, elles sont rendues infalsifiables et il ne fait aucun doute qu'elles proviennent de l'entité dont vous croyez qu'elles proviennent. D'un point de vue cryptographique, les objectifs d’authentification, d'intégrité, de confidentialité et de non-répudiation sont atteints.
* Respecte la vie privée - Dans les exemples présentés, nous voyons le titulaire (souvent aussi le sujet) d'un justificatif numérique contrôler les justificatifs et toutes les assertions établies sur la base de ces justificatifs. Nulle part nous ne voyons l'exigence absolue d'un fournisseur d'identité tiers responsable de la gestion du justificatif numérique, ni d'un vérificateur ayant le contrôle total d'un justificatif délivré. De même, nous constatons que seules les informations absolument nécessaires doivent être partagées. Enfin, nous constatons que l'émetteur n'est pas informé de l'utilisation du justificatif, ce qui renforce encore la protection de la vie privée. Ces caractéristiques des justificatifs vérifiables constituent une amélioration significative de la protection de la vie privée par rapport aux méthodes plus traditionnelles de gestion des justificatifs numériques.
* Vérifiable de façon automatisée - En utilisant des approches basées sur des standards qui s'appuient sur les techniques de cryptographie à clé publique et privée, toutes les assertions peuvent être systématiquement déchiffrées et facilement comprises sans avoir besoin d'interfaces propriétaires entre les participants d'un écosystème d'identité numérique.

### Identifiants décentralisés

Les exemples utilisés pour décrire les justificatifs vérifiables dépendent du *Verifiable Credentials Data Model* du W3C pour les schémas visant à capturer les données des justificatifs. Les exemples présentés précédemment dépendent également d'un autre standard émergent du W3C: [Decentralized Identifiers](https://w3c.github.io/did-core/) (DID ou « identifiants décentralisés »). Ce standard, toujours au stade de recommandation (mai 2021), définit un nouveau type d'identifiant unique et l'architecture pour sa mise en place. Certains éléments de cette architecture étaient présents dans les exemples utilisés dans la section précédente sur les justificatifs vérifiables.

Les [objectifs déclarés des identifiants décentralisés](https://www.w3.org/TR/did-core/#design-goals) sont les suivants :

* Éliminer l'exigence d'autorités centralisées ou d’un point de défaillance unique dans la gestion des identifiants, y compris l'enregistrement d'identifiants unique, vérification des clés publiques, de services et d'autres informations.
* Donner aux entités, humaines ou non, le pouvoir de contrôler directement leurs identifiants numériques sans avoir à s'en remettre à des autorités extérieures.
* Permettre aux entités de contrôler la confidentialité de leurs informations, y compris la divulgation minimale, sélective et progressive d'attributs ou d'autres données.
* Assurer une sécurité suffisante pour que les parties requérantes puissent compter sur les documents des identifiants décentralisés (*DID documents*) pour le niveau d'assurance requis.
* Permettre aux contrôleurs des identifiants décentralisés (*DID controllers*) de fournir une preuve cryptographique lorsqu'ils interagissent avec d'autres entités.
* Permettre aux entités de découvrir les identifiants décentralisés pour d’autres entités, pour en savoir plus sur ces entités ou interagir avec elles.
* Utiliser des standards interopérables afin que l'infrastructure des identifiants décentralisés puisse utiliser les outils existants et les bibliothèques de logiciels conçus pour l'interopérabilité.
* Être indépendant des systèmes (et des réseaux) et permettre aux entités d'utiliser leurs identifiants numériques avec tout système prenant en charge les identifiants décentralisés et les méthodes d’identifiants décentralisés (*DID methods*).
* Privilégier un ensemble réduit de fonctionnalités simples pour rendre la technologie plus facile à comprendre, à mettre en place et à déployer.
* Dans la mesure du possible, autoriser l'extensibilité, à condition qu'elle n'entrave pas trop l'interopérabilité, la portabilité ou la simplicité.

L'architecture d'un identifiant décentralisé comprend une référence au sujet (c'est-à-dire le sujet de l'identifiant), des localisateurs pointant vers des ressources clés (par exemple, une clé publique particulière associée aux données), les données associées à l'identifiant telles que les attributs ou les informations nécessaires pour localiser et utiliser les ressources requises pour utiliser l'identifiant, et des informations permettant d’identifier l'entité autorisée à maintenir un identifiant décentralisé. Cet ensemble d'informations est souvent stocké dans un registre de données vérifiable. Cependant, il existe des modèles qui permettent la communication pair à pair d'un identifiant décentralisé.

Si l'on examine les objectifs et les composants d'architecture des identifiants décentralisés, il apparaît que le standard vise à définir des identifiants indépendants et composés de toutes les informations à utiliser dans de nombreux scénarios de gestion d'identité numérique. *Il s'agit là d'un point important.* Les justificatifs vérifiables et les identifiants décentralisés aident à définir les standards en matière d'information et de structure de données pour permettre des modèles de gestion d'identité numérique comme le modèle pair à pair que nous avons défini dans un module d'apprentissage précédent. Toutefois, ces standards *ne prescrivent pas* un modèle ou une technologie de mise en place particulière. Ces standards peuvent être utilisés pour créer un [pont d'interopérabilité](https://www.w3.org/TR/did-core/#:~:text=The%20Decentralized%20Identifiers%20(DIDs)%20defined,identifiers%20using%20systems%20they%20trust.) entre les écosystèmes d'identité numérique centralisés ou fédérés existants et les modèles décentralisés, comme l'exemple utilisé dans la section sur les justificatifs vérifiables.

Pour illustrer, examinons un composant de l'architecture d'un identifiant décentralisé: le *registre de données vérifiables*. Le guide des standards le définit simplement comme toute forme de stockage de données. Il peut s'agir d'anciens systèmes d'identité numérique qui ont été développés pour prendre en charge les identifiants décentralisés. Outre les exigences en matière de données définies dans le standard du W3C, cela signifie également qu'il faut s'assurer que l’identifiant décentralisé est utilisable uniquement sur la base de la méthode et des informations de localisation qui font partie de l’identifiant décentralisé lui-même (c'est-à-dire qu'il faut supprimer toute exigence absolue concernant les systèmes propriétaires ou les fournisseurs d'identité).

En pratique, une grande partie du travail d'évolution dans le monde des justificatifs numériques se concentre actuellement sur des approches basées sur l'identité auto-souveraine, qui est abordée plus loin dans ce module d'apprentissage, et sur des technologies comme la technologie des registres distribués, qui comprend la chaîne de blocs, qui fournissent une architecture de service inclusive plus ouverte et promettent d'offrir une sécurité et une protection de la vie privée renforcées qui sont les objectifs de l’identifiant décentralisé.

### Vérifiez votre compréhension

Prenons un instant pour nous assurer que vous avez bien saisi les concepts que nous avons abordés jusqu'à présent. Dans cette activité, choisissez la meilleure réponse. Cette activité n'est pas chronométrée, alors n'hésitez pas à prendre votre temps pour la réaliser.

1. Un justificatif vérifié est simplement une assertion de justificatif présentée qui a fait l'objet d’une validation réussie.
2. Vrai
3. \*Faux
4. Les justificatifs vérifiables sont principalement pris en charge par deux standards développés par le World Wide Web Consortium (W3C).
5. \*Vrai
6. Faux
7. La définition d'un justificatif vérifiable est la suivante : un mécanisme permettant d'exprimer les justificatifs d'identité sur le Web d'une manière qui est cryptographiquement sécurisée, qui respecte la vie privée et qui est vérifiable de façon automatisée.
8. \*Vrai
9. Faux
10. Pour que les justificatifs vérifiables fonctionnent, ils doivent soutenir quatre acteurs différents. Lequel n'est pas l'un de ces acteurs?
11. Sujet
12. \*Assertion
13. Émetteur
14. Vérificateur
15. Titulaire
16. Le titulaire d'un justificatif vérifiable est toujours le sujet de ce justificatif.
17. Vrai
18. \*Faux
19. \_\_\_\_\_\_\_\_\_\_\_ est/sont utilisé(e)(s) pour le chiffrement et la signature numérique de l'«enveloppe» contenant le justificatif afin de s’assurer que le justificatif ne peut être utilisé que par le destinataire prévu (c'est-à-dire, le titulaire) et que le titulaire peut être assuré qu'il provient de l'émetteur.
20. La validation
21. \*La cryptographie
22. La vérification
23. Les identifiants
24. Une assertion vérifiable consiste en des données d’identification extraites d'un ou plusieurs justificatifs assemblés pour être présentés dans un contexte spécifique.
25. \*Vrai
26. Faux
27. Les identifiants décentralisés comportent un certain nombre d'objectifs déclarés. Ces objectifs comprennent lesquels des éléments suivants :
28. Donner aux entités, humaines ou non, le pouvoir de contrôler directement leurs identifiants numériques sans avoir à s'en remettre à des autorités extérieures.
29. Assurer une sécurité suffisante pour que les parties requérantes puissent compter sur les documents des identifiants décentralisés (*DID documents*) pour le niveau d'assurance requis.
30. Permettre aux entités de découvrir les identifiants décentralisés pour d’autres entités, pour en savoir plus sur ces entités ou interagir avec elles.
31. Privilégier un ensemble réduit de fonctionnalités simples pour rendre la technologie plus facile à comprendre, à mettre en place et à déployer.
32. \*Tous ces éléments sont inclus dans les objectifs
33. Les preuves cryptographiques d'un justificatif vérifiable sont enregistrées dans l'identifiant décentralisé.
34. \*Vrai
35. Faux
36. Un identifiant décentralisé contient tous les attributs importants du justificatif d'un justificatif vérifiable.
37. Vrai
38. \*Faux

## Entrevue avec des experts

## Conclusion

Les deux standards du W3C que nous avons brièvement explorés dans ce module d'apprentissage sont des éléments clés de l'évolution, au cours des dernières années, de l'approche de la création, de l'utilisation et de la gestion des justificatifs numériques. Alors que la communauté mondiale continue de développer les meilleures pratiques, standards et technologies pour la mise en œuvre de justificatifs vérifiables, le *Verifiable Credential Data Model* et les identifiants décentralisés soutiennent uniformément ces efforts de développement. Les modules d'apprentissage suivants exploreront certains des modèles de conception et des technologies fréquemment utilisés pour l'évolution des meilleures pratiques de mise en œuvre des justificatifs numériques pair à pair.

## Questionnaire du module 5

Vous n'avez qu'un seul essai pour répondre à ce questionnaire de quinze (15) questions sur le module. Ce questionnaire n'est pas chronométré, alors prenez votre temps pour examiner attentivement les options avant de choisir la meilleure réponse.

1. Un justificatif vérifié répond à des questions telles que « les informations présentées sont-elles exactes? Appartiennent-elles à la personne qui revendique cette identité? ».
   1. \*Vrai
   2. Faux
2. Un modèle qui prend en charge des justificatifs vérifiables doit prévoir \_\_\_\_\_\_\_\_\_\_\_\_\_ acteurs ou rôles.
   1. 3
   2. 4\*
   3. 5
   4. Aucune de ces réponses
3. L'entité ou la chose au sujet de laquelle une assertion est donnée.
   1. Émetteur
   2. \*Sujet
   3. Titulaire
   4. Vérificateur
   5. Demandeur
4. Les justificatifs vérifiables, tels que définis par le W3C, ne doivent pas nécessairement être vérifiables de façon automatisée.
   1. Vrai
   2. \*Faux
5. L'entité ou la personne qui vérifie l’assertion concernant un sujet donné.
   1. Émetteur
   2. Demandeur
   3. Titulaire
   4. \*Vérificateur
6. L'entité qui contrôle les justificatifs vérifiables.
   1. Émetteur
   2. Sujet
   3. \*Titulaire
   4. Vérificateur
7. Un justificatif vérifiable, comme tout justificatif, fait l'objet d'une validation et d'une vérification avant d'être délivré.
   1. \*Vrai
   2. Faux
8. Les standards du W3C tels que *Verifiable Credentials Data Model* et *Decentralized Identifiers* ne traitent pas des exigences technologiques pour la mise en œuvre.
   1. \*Vrai
   2. Faux
9. Les signatures numériques sont une exigence des justificatifs vérifiables.
   1. \*Vrai
   2. Faux
10. Les deux standards souvent cités lors de l'étude des justificatifs vérifiables et de l'identité décentralisée sont le standard *data model for verifiable credentials* et le standard *specification for decentralized identifiers* publiés par le/l’\_\_\_\_\_\_\_ .
    1. ISO
    2. \*W3C
    3. NIST
    4. IETF
    5. CCIAN
11. Il est nécessaire d'avoir une intégration « point à point » entre l'émetteur et le vérificateur.
    1. Vrai
    2. \*Faux
12. La possibilité d'extraire les informations nécessaires et de ne présenter que ces informations à l’utilisateur final est appelée \_\_\_\_\_\_\_.
    1. \* la divulgation sélective
    2. la cryptographie
    3. les identifiants décentralisés
    4. le *Verified credentials data model*
13. Parmi les choix suivants, quels sont les avantages des justificatifs vérifiables ?
    1. Le justificatif fournit une preuve cryptographique que le document est authentique
    2. Les informations n'ont pas été altérées
    3. Une méthode d'authentification forte de l'émetteur sans que celui-ci ait à participer à l'échange
    4. \*Toutes ces réponses sont des avantages
14. Qu'est-ce qui rend un justificatif vérifiable?
    1. La validation pour s'assurer que les informations sont exactes
    2. La vérification pour s'assurer qu'elles appartiennent à l'entité qui est le sujet d’un justificatif numérique
    3. \*a et b
    4. Aucune de ces réponses
15. \_\_\_\_\_ signifie que l’assertion ou le justificatif est signé et chiffré à l'aide des paires de clés publiques et privées des entités qui effectuent la transaction.
    1. \*Cryptographiquement sécurisé
    2. Respectueux de la vie privée
    3. Vérifiable de façon automatisée

# 

# Module 6: Considérations liées à la conception des solutions d'identité numérique

## Introduction

Dans ce module d'apprentissage, nous commençons à examiner de plus près les techniques particulières et les modèles de conception souvent utilisés lors de la création de systèmes de justificatifs numériques. Nous explorerons certaines des considérations et des choix importants à faire d'un point de vue des systèmes. Dans un module d'apprentissage ultérieur, nous examinerons certaines des technologies courantes utilisées pour mettre en place les conceptions.

Dans un monde où l'identité numérique est de plus en plus répandue et où la valeur des transactions effectuées par voie électronique continue d'augmenter, les menaces envers nos justificatifs et nos renseignements personnels continueront d'augmenter au même rythme. En nous appuyant sur notre examen des justificatifs vérifiables et de l'identité décentralisée, nous verrons comment l'utilisation de technologies et de techniques cryptographiques soutient l’interopérabilité entre les participants qui créent et utilisent des justificatifs numériques.

Dans un module d'apprentissage précédent, nous avons mentionné plusieurs des modèles d'architecture de service de haut niveau qui influencent la mise en place d'un écosystème d'identité numérique. Dans ce module, nous décrirons plusieurs techniques, technologies et éléments de conception de solutions qui sont de plus en plus utilisés pour mettre en œuvre des services liés aux justificatifs numériques.

Cette liste n'est pas exhaustive, nous avons sélectionné certaines des techniques les plus importantes disponibles dans le domaine public pour fournir un point de départ lors de la conception de solutions pour les justificatifs numériques.

## Objectifs d'apprentissage

1. Examiner la cryptographie
2. Décrire les principaux modèles de conception des justificatifs numériques
   1. Divulgation numérique sélective
   2. Preuve à divulgation nulle de connaissance
   3. Portefeuille numérique
   4. Identité auto-souveraine
   5. Trust over IP

## La cryptographie

### Introduction à la cryptographie

Nous avons vu l'importance de la cryptographie utilisée pour fournir certaines des capacités de base requises pour sécuriser un écosystème d'identité numérique. Lorsque nous réfléchissons à la cryptographie à utiliser et à la manière de l'utiliser, nous devons d'abord comprendre les types de services de sécurité que la cryptographie peut prendre en charge :

* La confidentialité est le service fondamental de la cryptographie. Le fait de bien chiffrer des informations sensibles permet de s'assurer qu'elles sont ne sont pas intelligibles pour des entités non autorisées;
* L'intégrité des données confirme que les informations n'ont pas été altérées depuis leur création;
* L'authentification permet de confirmer que l'information a été envoyée par l'expéditeur prévu; et
* La non-répudiation garantit que l'expéditeur ne peut pas désavouer ou nier la création d'un message chiffré.

La cryptographie à clé publique utilise des clés pour faciliter la signature ou le chiffrement des messages. Plus la clé et l'algorithme de chiffrement sont longs et complexes, moins il est probable qu'une entité non autorisée puisse déchiffrer ou signer faussement un message. La cryptographie est basée sur l'un des deux modèles de base:

1. Le chiffrement symétrique utilise la même clé pour chiffrer/déchiffrer un message.
2. Le chiffrement asymétrique utilise une clé pour chiffrer un message et une autre clé mathématiquement liée pour le déchiffrer.

Le chiffrement symétrique est plus facile à exécuter, consommant moins de ressources informatiques, ce qui rend ce modèle bien adapté au chiffrement à l'intérieur d'un réseau fermé ou entre deux parties bien connues l'une de l'autre. Les inconvénients de cette approche sont notamment la difficulté de s'assurer que les deux parties disposent de la même clé, et la difficulté de vérifier l'origine d'un message reçu. En outre, cryptographie symétrique n'est pas très évolutive. Elle peut fonctionner correctement pour les échanges entre deux parties qui ont une confiance préétablie, mais lorsque le nombre de parties augmente, les difficultés liées à la gestion des clés augmentent de manière exponentielle. Le chiffrement symétrique est souvent utilisé dans des réseaux fermés sur de grands volumes d'informations. On peut citer comme exemple le chiffrement de bases de données ou de grands volumes de données échangées sur un réseau fermé (par exemple, dans le secteur financier).

Dans le monde en ligne, les échanges protégés sur l'Internet ouvert entre des parties qui n'ont pas de relation de confiance préétablie entre leurs systèmes sont fréquents. C'est pourquoi le chiffrement qui repose en grande partie sur la cryptographie asymétrique est plus souvent utilisé. Le chiffrement asymétrique utilise des paires de clés qui sont mathématiquement liées. Une clé est utilisée pour chiffrer un message, et seule l'autre clé peut le déchiffrer. C'est la base du chiffrement à clé publique . Dans le chiffrement à clé publique, l'une des paires de clés est rendue publique, tandis que l'autre reste privée et protégée.

Il est possible que ces paires de clés soient auto-générées ; l'infrastructure à clé publique (ICP) introduit une autorité de certification de confiance chargée de délivrer les certificats numériques utilisés pour générer les paires de clés. Ces autorités de certification jouent deux rôles principaux:

1. Tout d'abord, elles s'assurent que le certificat est délivré selon un ensemble bien établi de règles de validation afin de garantir que le certificat est délivré à une entité connue et installé comme prévu.
2. Deuxièmement, elles maintiennent une liste de révocation qui peut être consultée à tout moment pour s'assurer que le certificat délivré est valide. Il s'agit d'un rôle important qui prend en charge la fonction d'authentification dans la cryptographie, en créant essentiellement un tiers de confiance qui peut attester de l'authenticité des clés publiques.

NOTE : nous mentionnons les autorités de certification et l'ICP pour souligner l'origine de la partie «I» de l'ICP (c'est-à-dire l'infrastructure). L'utilisation de la cryptographie à clé publique dans les modèles de justificatifs numériques ne nécessite pas d'autorités de certification comme c'est le cas pour l'ICP.

### Le chiffrement asymétrique en action

Voyons un exemple de chiffrement asymétrique en action. La vidéo ci-dessous montre un échange entre John et Sally utilisant la cryptographie à clé publique pour fournir les quatre services de sécurité (c'est-à-dire la confidentialité, l'authentification, l'intégrité des données et la non-répudiation), que nous avons mentionnés précédemment.

<<Explainer video goes here>>

### Approches de chiffrement

Le chiffrement (quel que soit le modèle) dépend de l'algorithme qui est utilisé pour chiffrer les informations. L'algorithme est généralement plus ou moins sécurisé en fonction de la longueur de la clé utilisée pour «alimenter» l'algorithme.

Alors, pourquoi ne pas rendre la clé aussi longue que possible? Une clé plus longue entraîne un compromis en termes de performance, car une plus grande puissance de traitement est requise pour chiffrer et déchiffrer les informations. Les algorithmes les plus couramment utilisés aujourd'hui sont l'*Advanced encryption system* (AES) proposé par le [NIST](https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines) et l'algorithme de chiffrement asymétrique RSA ([*RSA asymmetric encryption algorithm*](https://datatracker.ietf.org/doc/html/rfc8017)). Ces deux algorithmes permettent d'utiliser différentes longueurs de clé et, ainsi, ils offrent la possibilité d'adapter la cryptographie à différents niveaux de risques ou de performance. Les algorithmes et les standards pour leur utilisation évoluent constamment, tout comme les capacités d’attaques malveillantes de sécurité.

Enfin, il existe un modèle mixte qui est souvent employé en cryptographie pour tirer parti des forces des approches symétriques (rapidité et efficacité) et asymétriques (meilleur soutien à la confiance). Dans cette approche, les méthodes asymétriques sont utilisées pour établir une base de confiance pour l'interaction et les clés symétriques sont générées pour être utilisées dans la transaction à protéger.

Prenons un exemple.

L'une des utilisations les plus courantes de cette approche est l'établissement d'une session de navigation sécurisée. Pour établir une connexion sécurisée avec un navigateur, le navigateur et le serveur internet s'identifient mutuellement en utilisant un échange asymétrique de clés. Cela permet d'exploiter les fonctions d'authentification des méthodes asymétriques. Au cours de cet échange, une clé à usage unique est générée et partagée entre le serveur internet et le navigateur. À partir de ce moment, et jusqu'à la fin de la session de communication, cette clé générée et le chiffrement symétrique sont utilisés. Cela présente l'avantage de tirer parti de la rapidité du chiffrement symétrique pour les échanges d'informations volumineux entre le navigateur et le serveur internet.

### Signatures numériques

La cryptographie à clé publique est également utilisée pour les signatures numériques, un composant important des modèles d'identité décentralisés. Les signatures numériques prouvent qu'un message numérique n'a pas été modifié depuis qu'il a été signé. Le message à signer est pris et un condensé du message, court et unique, est créé et chiffré à l'aide de la clé privée de l'expéditeur. Le condensé du message (ou le « hachage ») généré est unique pour le message ou le document, et la modification de n'importe quelle partie de celui-ci changera complètement le hachage.

Lorsque le destinataire reçoit le message et la signature, il peut générer son propre hachage du message et déchiffrer le hachage de l'expéditeur (inclus dans le message original) à l'aide de la clé publique de l'expéditeur. Le destinataire peut comparer le hachage qu'il a généré avec le hachage déchiffré. S'ils correspondent, le message n'a pas été modifié et l'expéditeur est authentifié puisque seule la clé publique de l'expéditeur aurait pu déchiffrer un hachage généré par la clé privée de l'expéditeur.

## La divulgation sélective

### Introduction à la divulgation sélective

Maintenant que nous avons exploré les approches émergentes qui présentent des justificatifs vérifiables et des modèles distribués, le reste de ce module définira et décrira les approches souvent considérées comme « la voie à suivre ». La plupart de ces approches ne sont pas incompatibles. Il s'agit plutôt d'éléments d'un écosystème d'identité global amélioré qui institue un meilleur contrôle de l'utilisateur sur les justificatifs numériques, une divulgation limitée (telle que définie dans les 10 principes relatifs à l'équité dans le traitement de l'information) et une moins grande dépendance à l'égard des technologies propriétaires et des fournisseurs de services.

La divulgation sélective, une fonction importante pour faciliter la divulgation minimale d'informations, est un terme souvent employé pour décrire les meilleures pratiques d’utilisation des justificatifs numériques. La divulgation sélective est la capacité d’un sujet de partager un sous-ensemble déterminé d'informations, limitée aux seules informations requises à un moment donné. Du point de vue des justificatifs numériques, cela signifie la capacité de partager uniquement les **identifiants** et **attributs** des justificatifs nécessaires pour établir l'identité dans un contexte spécifique. La capacité de divulguer de manière sélective des renseignements personnels en fonction des informations réellement requises par un utilisateur final est un élément particulièrement important de la protection de la vie privée dès la conception.

### Exemple de divulgation sélective

Un exemple souvent utilisé pour illustrer ce concept est la vérification de l'âge pour entrer dans un bar. Examinons de plus près cet exemple pour illustrer le concept de la divulgation sélective.

Dans cet exemple, un permis de conduire sera utilisé pour vérifier l'identité et l'âge. Votre permis de conduire, qui est un justificatif d'identité, contient les informations suivantes :

* Nom
* Adresse
* Photo
* Taille
* Couleur des yeux
* Date de naissance
* Dates de délivrance et d'expiration

À la porte du bar, on vous demande de prouver que vous avez atteint un certain âge. Vous présentez votre permis de conduire et votre photo est utilisée pour vérifier si le justificatif vous appartient. Votre date de naissance est utilisée pour déterminer si vous avez l'âge pour entrer. Malheureusement, vous avez également révélé des renseignements personnels sensibles qui n'étaient pas nécessaires (par exemple, l'adresse de votre domicile). Plus inquiétant encore, les documents d'identité sont souvent scannés dans ce scénario, ce qui signifie que vous avez également renoncé au contrôle de ces informations.

Si la divulgation sélective était possible dans ce scénario, vous auriez dû être en mesure d'exposer uniquement votre photo et votre date de naissance lorsqu'on vous a demandé votre identité pour entrer dans le bar.

Du point de vue de l'identité numérique, l'approche de la divulgation sélective s'est largement concentrée sur l'utilisation des techniques de signature numérique pour n'exposer que les identifiants ou les attributs nécessaires, tout en gardant les informations superflues inaccessibles. Par exemple, si l'on se réfère aux méthodes examinées dans le domaine de la cryptographie asymétrique, on pourrait reproduire la signature de chaque attribut du justificatif et permettre la sélection de ces éléments de données plus granulaires dans une assertion d'identité.

Il existe plusieurs conditions préalables pour permettre la divulgation sélective, notamment :

* la construction d'un justificatif sous une forme qui permet la divulgation sélective;
* la technologie, la cryptographie et les processus qui permettent la divulgation sélective;
* la capacité des vérificateurs de justificatifs à formuler la demande d'informations appropriée pour ne demander que ce qui est nécessaire (par exemple: « J'ai besoin d'une photo et d'une confirmation de l'âge à partir d'une identité délivrée par le gouvernement »); et
* la possibilité de vérifier la réponse reçue à la demande.

Les standards pour les justificatifs vérifiables et les identifiants distribués abordés précédemment dans ce module d'apprentissage constituent une base pour la mise en place de la divulgation sélective, ouverte et basée sur des standards.

Revenons un instant à notre exemple. Nous avons décrit un scénario dans lequel la photo et la date de naissance étaient partagées. En fait, la date de naissance n'était pas ce qui était réellement requis. Ce qui était requis, c'était une assertion de confiance indiquant que la personne avait dépassé un certain âge. Les standards que nous avons examinés précédemment permettent également d'envisager la création sur demande d'une assertion vérifiable de « j'ai dépassé l'âge requis ». Cela nécessiterait des systèmes qui posent la bonne question (par exemple : « La date de naissance est-elle supérieure au minimum requis? ») et des processus qui permettraient la construction d'une assertion vérifiable qui répondrait directement à la demande. Dans les cas où la date de naissance, et uniquement la date de naissance, a été partagée, il s'agit d'une divulgation sélective. Une technique que nous explorerons plus tard, appelée la preuve à divulgation nulle de connaissance, étend ceci en établissant une assertion vérifiable qui prouve l'âge sans révéler la date de naissance.

Des travaux sont en cours dans le domaine de la cryptographie, de la technologie et des processus technologiques pour mettre au point des approches qui permettraient d'atteindre cet objectif. Cependant, une condition préalable à l'utilisation à grande échelle de cette approche idéale de la divulgation sélective nécessitera l'utilisation généralisée de certains des standards sous-jacents (par exemple, *Verifiable Credentials*, DID) qui rendent possibles des approches comme celle-ci. De même, les standards technologiques ouverts utilisés pour construire et consommer des justificatifs vérifiables permettant une divulgation sélective à ce niveau devront être utilisés pour construire les solutions techniques accompagnant le portefeuille numérique et les systèmes internes du vérificateur.

Nous approfondirons ce point dans un module d'apprentissage ultérieur, où nous examinons certaines des technologies utilisées pour mettre en place des justificatifs vérifiables.

## Divulgation nulle de connaissance

### Introduction à la preuve à divulgation nulle de connaissance

Bon nombre des transactions que nous effectuons nécessitent la divulgation de renseignements personnels. Cela est particulièrement pertinent pour la création ou l'utilisation de justificatifs numériques. Les preuves à divulgation nulle de connaissance permettent de vérifier que vous savez quelque chose, sans révéler exactement ce que c'est. Cela permet de contourner de nombreux problèmes de protection de la vie privée présents dans notre monde en ligne actuel. La connaissance n'est pas exposée sous sa forme réelle sur l'internet, tandis que les vérificateurs peuvent être certains que l'entité avec laquelle ils traitent possède la connaissance, l'attribut ou le secret, dont ils ont besoin.

Nous verrons plus tard comment cela peut s'appliquer à des authentifiants comme un mot de passe, alors prenons cet exemple. Lorsque vous utilisez un mot de passe pour vous authentifier, le vérificateur n'a pas nécessairement besoin que vous entriez le mot de passe - il doit savoir que vous connaissez le mot de passe! La preuve à divulgation nulle de connaissance fournit un mécanisme permettant de déterminer cette connaissance sans que vous ayez à la saisir et à la transmettre dans un environnement qui pourrait être soumis à des acteurs malveillants tentant de voler ce secret. Un autre exemple pourrait être de montrer que vous vivez au Canada sans divulguer l'endroit exact où vous vivez, ou que votre score de crédit est supérieur à 600, etc.

Il existe quelques exemples non numériques couramment utilisés pour démontrer ce concept. Celui que je préfère est le cas où deux personnes, dont l'une est daltonienne, disposent de deux balles de couleur.

Le daltonien ne peut pas distinguer les balles, alors que l'autre personne peut. Le daltonien cache les deux balles derrière son dos et choisit au hasard de les échanger ou non. Il tend ensuite sa main droite et demande si les balles ont été échangées. L'autre personne peut savoir, d'après la couleur de la balle présentée, si elles ont été échangées et répondre en conséquence. En faisant cet exercice une fois, il y a 50% de chances que la réponse soit correcte en avançant une supposition. Cependant, si cet exercice était répété, les chances d'obtenir la bonne réponse à *chaque fois* diminueraient.

En répétant suffisamment l'exercice, les chances que l'autre personne ait raison à *chaque fois* seraient près de zéro. C'est l'essence même de la preuve à divulgation nulle de connaissance. Une personne a démontré qu'elle savait si les balles avaient été échangées sans révéler aucune autre information sur les balles. En ce qui concerne le daltonien, il ne sait rien de plus sur les balles qu'au départ, mais il sait que l'autre personne connaît les balles et sait si elles ont été échangées.

### Critères de la preuve à divulgation nulle de connaissance

Une preuve à divulgation nulle de connaissance doit répondre à trois critères :

* Intégralité - Lorsqu'une déclaration est vraie, le vérificateur sera convaincu de ce fait.
* Robustesse - Aucune supposition aléatoire ou autre approche malveillante pour faire une déclaration vraie n'est possible, avec une quasi-certitude.
* Connaissance nulle - Si la déclaration est vraie, le vérificateur n'apprend rien d'autre que le fait que la déclaration est vraie.

Comment tout cela fonctionne-t-il dans un monde en ligne? Comme nous l'avons vu précédemment, la science des probabilités est un élément clé. Si une réponse correcte peut être fournie à chaque fois, le vérificateur peut avoir la certitude statistique que la personne possède les connaissances demandées. Mais comment révéler la possession de connaissances sans révéler les connaissances elles-mêmes dans un monde en ligne?

Pour ce faire, des mathématiques et des techniques de chiffrement très avancées sont utilisées. Si les entrées d'un algorithme complexe sont la valeur numérique d'un secret ou d'une connaissance détenue + un nombre aléatoire, les résultats de l'algorithme peuvent être envoyés à un vérificateur et celui-ci peut déterminer si la « réponse » exige la possession de la connaissance qu'il veut vérifier. Si ce processus est répété suffisamment de fois et que la réponse démontre toujours la possession des connaissances, la loi des probabilités permet au vérificateur d'être statistiquement certain que la personne à qui il a affaire a effectivement la connaissance du secret.

Dans un cas d'utilisation pratique, cette approche peut consister à poser une question comme : « Êtes-vous un résident de la Nouvelle-Écosse? » et à alimenter l'algorithme avec la valeur de votre code postal pour fournir une série de réponses qui ne sont possibles que si votre code postal est valide et commence par la lettre « B ». Dans ce scénario, le vérificateur est certain que vous êtes un résident en Nouvelle-Écosse, mais il ne reçoit pas votre adresse exacte ou aucune partie de celle-ci (comme c'est le cas dans de nombreux cas actuellement). La protection de la vie privée est maximisée et la confiance nécessaire au vérificateur est satisfaite.

On peut se demander quelle est l'efficacité de ce processus lorsqu'il doit être répété suffisamment de fois pour fournir une certitude statistique. Plusieurs techniques présentant un degré de complexité important sont avancées dans ce domaine. Nous n'entrerons pas dans les détails de celles-ci ici. Il existe une autre approche applicable lorsque les deux parties possèdent la connaissance, ce qui nous ramène à l'exemple des mots de passe. Les deux parties connaissent la valeur d'un authentifiant, comme un mot de passe, mais souhaitent éviter les problèmes de sécurité associés à la transmission de la valeur du mot de passe pendant l'authentification.

Dans ce cas, des mathématiques complexes peuvent être utilisées pour générer des modèles qui sont générés avec la valeur du mot de passe. Si plusieurs modèles sont produits en utilisant la même « valeur initiale » et comparés à un modèle généré par le vérificateur, les mathématiques complexes dont nous avons parlé peuvent être utilisées pour déterminer si tous les modèles produits doivent provenir de la même source. Ce processus est nettement plus succinct et offre le même niveau de confiance dans les connaissances détenues.

## Portefeuilles numériques

### Portefeuilles numériques

Dans un monde physique, nous stockons la plupart de nos justificatifs dans un portefeuille physique. L'objectif d'un portefeuille numérique n'est pas différent. Il s'agit de quelque chose qui est facilement accessible et qui peut stocker plusieurs justificatifs (par exemple, un permis de conduire, des cartes de crédit) et authentifiants (par exemple, des cartes à puce), et les protéger de la ligne de mire immédiate.

Les tentatives de création de portefeuilles numériques existent depuis des années. Avec l'arrivée des améliorations apportées à la technologie des téléphones intelligents, nous avons assisté à une explosion de l'utilisation des portefeuilles numériques pour le paiement (pensez à Google Pay ou Apple Pay). De plus, les portefeuilles numériques sont un composant clé pour la gestion de la cryptomonnaie. Cependant, beaucoup de ces portefeuilles sont conçus pour des types d'utilisation limités (par exemple, les transactions financières) et beaucoup sont basés sur des systèmes propriétaires ou des réseaux. Le concept du portefeuille numérique, appliqué à la gestion d'identité basée sur des standards, présente des exigences que de nombreux portefeuilles financiers ou de cryptomonnaies ne remplissent pas à l'heure actuelle.

### Qu'est-ce qu'un portefeuille numérique et comment fonctionne-t-il?

Prenons un peu de recul. Qu'est-ce que le portefeuille numérique et comment fonctionne-t-il?

Un portefeuille numérique est un logiciel conçu pour contenir et sécuriser les informations nécessaires pour effectuer une transaction. Il peut s'agir d'informations telles que des informations financières (semblables à celles contenues sur votre carte de crédit), des justificatifs numériques (comme ceux dont nous avons discuté tout au long des modules d'apprentissage) ou des clés cryptographiques (utilisées pour déverrouiller des données sensibles). Un portefeuille numérique peut prendre plusieurs formes : il peut s'agir d'un objet physique autonome avec un logiciel intégré (par exemple, une clé USB), ou d'un logiciel qui peut être hébergé sur un appareil dont vous avez le contrôle (par exemple, votre ordinateur ou votre téléphone intelligent), ou encore il peut être basé sur un logiciel que vous confiez à un fournisseur de services pour qu'il en assure la garde. Examinons quelques exemples concrets courants :

1. Matériel - De nombreux portefeuilles conçus pour gérer la cryptomonnaie sont intégrés à un dispositif de stockage USB. Cela présente l'avantage d'être portable et de fonctionner sur tout ce qui possède une interface USB (ordinateur, téléphone, etc.). Lorsque ces portefeuilles contiennent des cryptomonnaies, ils sont parfois appelés «portefeuilles de stockage à froid» («*cold storage wallets*»).
2. Basé sur un logiciel, contrôle local - L'exemple qui vient à l'esprit de la plupart des gens est le portefeuille numérique Apple Pay ou Google Pay utilisé pour les transactions financières. Il est généralement installé sur votre téléphone intelligent et accessible par des authentifiants activés sur votre téléphone intelligent (empreinte digitale, *scan* de l'iris, codes d'accès, etc.).
3. Basé sur un logiciel, hébergé par un fournisseur de services - Un exemple serait un courtier en cryptomonnaies qui fournit un portefeuille numérique dans le cadre d'un ensemble de services en ligne connexes (Coinbase est l'un des nombreux exemples).

Pour la suite de cette étude des portefeuilles numériques, nous partirons du logiciel de portefeuille numérique le plus utilisé, celui que vous installez sur votre téléphone intelligent.

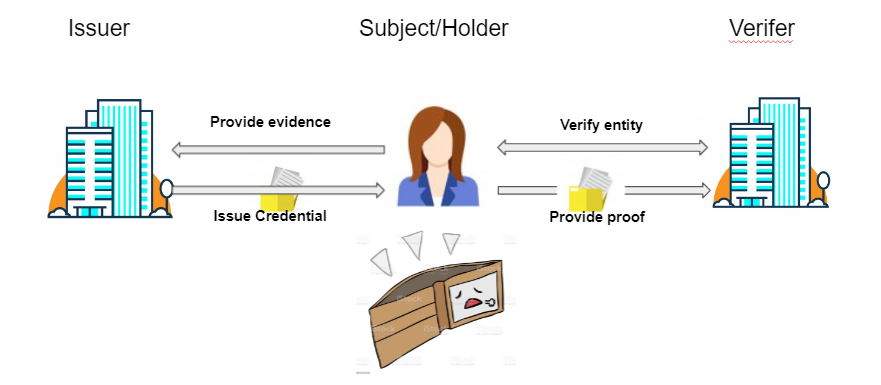
### Exemple de portefeuille numérique

L'image ci-dessous illustre l'utilisation possible d'un portefeuille numérique. Vous remarquerez qu'elle est similaire à la manière dont nous avons présenté le modèle pair à pair pour la gestion de justificatifs numériques dans un module d'apprentissage précédent. Un portefeuille numérique, ou un mécanisme similaire, est l'essence même d'un modèle de justificatifs numériques pair à pair.

Dans sa forme la plus simple, un portefeuille numérique présente deux interactions distinctes de base:

1. Délivrance:
   1. Le titulaire demande un justificatif et fournit une preuve d'identité selon les procédures établies par l'émetteur.
   2. L'émetteur construit et délivre ensuite un justificatif numérique vérifiable que le titulaire stocke dans son portefeuille numérique.
2. Présentation
   1. L'émetteur demande des informations des justificatifs au titulaire et le consentement du titulaire est requis.
   2. Le titulaire établit une assertion vérifiable à partir du ou des justificatifs contenus dans son portefeuille numérique et la présente au vérificateur.

Pour qu'un modèle pair à pair soit possible, ces justificatifs doivent être basés sur des standards, en utilisant des standards tels que *Verifiable Credentials* et *Distributed Identifiers* discutés précédemment. Une fois le justificatif délivré et en possession du titulaire, il peut être utilisé dans une interaction avec n'importe quel vérificateur équipé pour utiliser ce justificatif basé sur des standards. Lorsque le titulaire souhaite accéder aux services en ligne du vérificateur, il lui suffit de fournir le justificatif ou la « preuve » au vérificateur, ou lui en fournir une partie. En utilisant les méthodes que nous avons explorées avec les justificatifs vérifiables et les identifiants distribués, ainsi que la cryptographie à clé publique décrite précédemment, le vérificateur peut vérifier le justificatif. Si le vérificateur a choisi de faire confiance aux justificatifs délivrés par l'émetteur, aucune autre vérification ou consultation de tiers n'est nécessaire.



Les portefeuilles de justificatifs numériques efficaces devraient présenter toutes les caractéristiques suivantes :

* Le portefeuille est contrôlé par le titulaire et ne peut être vu, modifié ou retiré sans le consentement du titulaire. Ceci s'applique à tous, même au fabricant du portefeuille;
* Il est portable;
* Il est basé sur des standards;
* Il peut être rempli avec n'importe quel bien numérique qui respecte les standards;
* Il peut être remplacé par un autre portefeuille et son contenu est transférable à tout autre portefeuille basé sur des standards;
* Le portefeuille est sécurisé par des authentifiants que le titulaire contrôle;
* Les justificatifs perdus ne peuvent pas être récupérés, et ils doivent être recréés lors d'une interaction avec l'émetteur;
* Les émetteurs peuvent révoquer les justificatifs, mais ceux-ci restent, dans leur état révoqué, avec le titulaire; et
* Le titulaire a un contrôle total sur ce qui est partagé et avec qui.

Plus tôt, nous avons mentionné que les portefeuilles numériques utilisés à des fins d'identité présentent certaines caractéristiques qui ne sont pas présentes dans les portefeuilles apparus, au départ, pour l'utilisation lors de transactions financières ou la gestion de cryptomonnaies. De manière générale, ces caractéristiques sont:

* La mise en place de standards ouverts qui soutiennent des justificatifs vérifiables;
* L'interaction pour demander et communiquer le consentement au partage d'informations;
* Les concepts qui soutiennent la divulgation sélective ou le partage des composants d’un justificatif; et
* La présence d'un agent, une extension logicielle, qui peut établir des connexions et effectuer des échanges de justificatifs sur la base de standards ouverts pour les justificatifs vérifiables.

### Vérifiez votre compréhension

Instructions : Dans cette activité, vous devrez choisir entre vrai et faux pour la question associée. Lorsque vous aurez terminé, sélectionnez « Soumettre » en bas de la page.

1. Le chiffrement symétrique dépend des paires de clés de chiffrement. (faux)
2. Le chiffrement/déchiffrement symétrique nécessite moins de ressources informatiques. (vrai)
3. Le chiffrement à clé publique ou chiffrement asymétrique décrit une méthode, tout algorithme de chiffrement peut être utilisé. (vrai)
4. La divulgation sélective consiste à envoyer uniquement les données dont le vérificateur a besoin. (faux)
5. La divulgation sélective consiste à ne révéler que les données dont le vérificateur a besoin. (vrai)
6. La preuve à divulgation nulle de connaissance nous indique que la valeur d'un attribut d'identité est exacte. (faux)
7. La preuve à divulgation nulle de connaissance nous indique que l'assertion du titulaire est vraie sans révéler la valeur réelle de l'attribut du justificatif (vrai)
8. La preuve à divulgation nulle de connaissance fournit une certitude statistique de la véracité d'une assertion, et non une certitude absolue. (vrai)
9. Un portefeuille numérique est toujours détenu par le titulaire, et non par un fournisseur. (faux)
10. Les portefeuilles de paiement ou de cryptomonnaies soutiennent intrinsèquement les justificatifs vérifiables. (faux)
11. Un portefeuille numérique, ou un mécanisme similaire, est essentiel au modèle d'écosystème d'identité numérique pair à pair. (vrai)

## Identité auto-souveraine

### Introduction à l'identité auto-souveraine

L'auto-souveraineté est un terme que beaucoup auront entendu récemment. Il s'agit d'une approche en matière de justificatifs numériques qui remet davantage le contrôle de l'identité entre les mains de l'individu.

Plusieurs des concepts que nous avons présentés dans ce module d'apprentissage se combinent pour fournir les fondements de l'identité auto-souveraine (IAS). Il est généralement admis que l’IAS repose sur le contrôle par l'utilisateur de justificatifs vérifiables qui ne peuvent être partagés sans son consentement explicite. Cela implique quelques autres principes, comme l'absence d'exigence absolue d'autorités centralisées qui contrôlent la gestion ou l'utilisation de justificatifs numériques.

L'IAS est un développement relativement récent, généralement reconnu comme ayant été lancé avec la publication des [10 principes de l'identité auto-souveraine](https://github.com/WebOfTrustInfo/self-sovereign-identity/blob/master/self-sovereign-identity-principles.md) en 2016. Depuis, la communauté mondiale a collaboré pour faire évoluer les concepts pour l’établissement d'écosystèmes d'identité numérique basés sur l'IAS. Ces efforts de collaboration sont trop nombreux pour être couverts dans leur intégralité, mais plusieurs d'entre eux seront cités en exemple dans cette section.

L'IAS repose sur plusieurs fondements essentiels, dont les suivants:

* Les cadres de confiance et de gouvernance dans lesquels opère l'IAS
* Les principaux rôles requis dans l'écosystème de l'identité numérique (émetteur, titulaire et vérificateur).
* Un format de justificatif vérifiable
* Des identifiants distribués qui permettent la vérification sans avoir recours à des autorités centralisées
* Des éléments technologiques clés qui permettent l’implémentation
  + Portefeuilles numériques permettant de détenir en toute sécurité des justificatifs vérifiables.
  + Technologie ayant recours aux agents (*Agent technology)* permettant l'utilisation d'un justificatif vérifiable
  + Registres distribués (c'est-à-dire la chaîne de blocs) qui servent de sources de référence ouvertes et disponibles (à grande échelle) pour les identifiants distribués et les clés de chiffrement/déchiffrement nécessaires pour sécuriser les informations échangées au sein de l'écosystème.

Examinons de plus près chacun de ces éléments constitutifs.

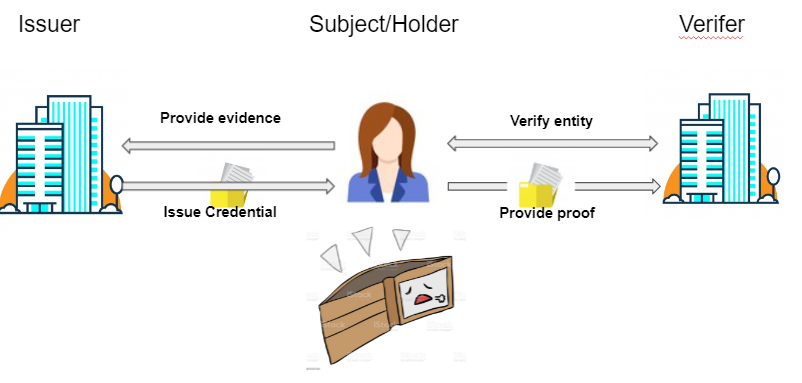
### Gouvernance

Comme nous l'avons appris, un écosystème d'identité numérique est régi par un ensemble de règles juridiques, de processus et de technologies qui représentent les exigences de participation. Certaines de ces règles sont établies par des organismes de réglementation ou de standardisation, tandis que d'autres sont définies dans les limites de l'écosystème lui-même. Les standards et les cadres de confiance qui constituent la base de la gouvernance forment la fondation sur laquelle repose un écosystème d'identité numérique sain.

Pour l'IAS, plusieurs travaillent activement à l'élaboration d'exigences en termes des meilleures pratiques pour la participation à un écosystème d’IAS. Les organismes internationaux de collaboration comprennent des influenceurs clés comme l'[Open Identity Exchange](https://openidentityexchange.org/) (OIX), la [Decentralized Identity Foundation](https://identity.foundation/) (DIF) et le [W3C](https://www.w3.org/). En outre, plusieurs gouvernements travaillent activement au développement et à l'adaptation de leurs standards et de leurs cadres de confiance pour inclure l'IAS. Les travaux sur des standards et des cadres de référence tels que le [CCP](https://diacc.ca/fr/), eIDAS et son cadre [ESSIF](https://essif-lab.eu/), ainsi que les standards technologiques connexes provenant d'organisations comme le [NIST](https://www.nist.gov/) sont mentionnés dans d'autres modules d'apprentissage. Ces activités juridictionnelles sont en cours et évoluent rapidement.

### Définition des rôles clés

L'IAS, dans sa forme la plus élémentaire, définit trois rôles principaux impliqués dans la délivrance et l'utilisation d'un justificatif vérifiable.

1. Un émetteur responsable de la délivrance d'un justificatif vérifiable.
2. Un titulaire qui acquiert, stocke et présente un justificatif vérifiable.
3. Un vérificateur qui vérifie le justificatif présenté.

Le modèle de base ne comporte aucune autorité centralisée susceptible de contrevenir aux standards de protection de la vie privée ou de devenir un point d'attaque attrayant pour les acteurs malveillants qui cherchent à voler des identités. Les barrières à l'adoption sont également plus faibles, car les intégrations entre l'émetteur et le vérificateur, ou un fournisseur de services d'identité, ne sont pas nécessaires. Plus loin dans cette section, lorsque nous examinerons certaines des composantes technologiques de base de l’IAS, nous verrons comment cela est possible.

### Un justificatif vérifiable

Un justificatif vérifiable est l'équivalent numérique d'un justificatif physique que nous transportons dans un portefeuille. Il s'agit de la forme et du format de base d'un justificatif numérique dans un écosystème d’IAS. Pour être utile au-delà d'un seul écosystème d'identité numérique, il doit suivre un format standard, où ce standard a été largement reconnu. Dans ce cas, la communauté mondiale des justificatifs numériques s'est ralliée autour du *Verifiable Credentials Data Model* du W3C, décrit plus haut dans cette section.

### Identifiants distribués

Un standard sur les justificatifs vérifiables nous indique comment formuler un justificatif, essentiellement la syntaxe requise pour exprimer un justificatif vérifiable. Cela ne crée pas *un standard pour l'utilisation d'un justificatif vérifiable*. C'est là que les identifiants distribués entrent en jeu.

Une approche standard des identifiants distribués permet une approche évolutive pour permettre la vérification d'un justificatif. Cela inclut des méthodes pour écrire, lire, mettre à jour et désactiver un identifiant. Les identifiants distribués pour les IAS ont également semblé se rallier autour d'un standard de base en cours de développement, à savoir le standard *Decentralized Identifiers* du W3C, décrit précédemment dans cette section. Ce standard constitue la base de l'approche et plusieurs organismes de standardisation collaboratifs l'utilisent actuellement comme point de départ pour étendre le modèle et le juxtaposer à des approches de chiffrement précises, à des standards de registres distribués et à un mélange d'autres techniques que nous avons explorées précédemment, comme la preuve à divulgation nulle de connaissance et des méthodes de divulgation sélective plus précises.

Les identifiants distribués introduisent une autre exigence absolue dans l'architecture de l’IAS. Il s'agit du registre distribué, qui fournit un registre de données vérifiable, généralement configuré pour être également ouvert et accessible. Ce registre est le plus souvent basé sur la technologie des chaînes de blocs. Nous verrons comment cela fonctionne un peu plus loin dans cette section.

### Portefeuilles numériques

Enfin, examinons certaines des composantes technologiques présentes dans presque toutes les descriptions de l'architecture d'un écosystème d'identité numérique basé sur l’IAS. Il s'agit des portefeuilles numériques, utilisés pour stocker en toute sécurité des justificatifs vérifiables, des agents logiciels permettant l'utilisation d'un justificatif vérifiable sur la base des standards, et des registres distribués qui sont au cœur de la capacité de l'IAS à fournir des services de confiance sans avoir besoin d'une autorité d'identité centralisée ou d'un fournisseur de services centralisé.

Du point de vue de l'IAS, il existe certaines [exigences clés](https://diacc.ca/wp-content/uploads/2020/12/Making-Sense-of-Digital-Wallets_FR.pdf) qui peuvent ne pas être présentes dans tous les produits de portefeuille numérique sur le marché :

* La mise en place de standards ouverts pour les justificatifs vérifiables portables;
* Fonctionne avec un logiciel ayant recours aux agents (*agent software*) qui permet l'échange et la vérification de justificatifs vérifiables;
* Devrait accepter tout justificatif vérifiable basé sur des standards et correctement constitué;
* Peut être installé sur plusieurs appareils (ordinateur, téléphone intelligent, etc.) et dispose de mécanismes pour rester synchronisé lorsqu'il est installé sur plusieurs appareils;
* Peut être sauvegardé et déplacé vers un autre portefeuille conforme aux standards (c'est-à-dire «débarré»); et,
* Offre la même expérience utilisateur de base que tout portefeuille conforme aux standards.

Le marché n'en est qu'à ses débuts et certaines caractéristiques, telles que la portabilité et la synchronisation, continueront d'évoluer à mesure que le marché se développera.

### Agents logiciels

Le portefeuille numérique est l'endroit où vos justificatifs vérifiables et vos clés cryptographiques privées sont stockés, en utilisant des formats basés sur des standards largement adoptés. Cependant, ce n'est que la moitié de l'équation. Pour être utile, le justificatif doit être géré de manière sécurisée pendant la présentation et la vérification. En outre, comme l'IAS s'appuie sur des standards, cette interaction entre l'émetteur et le titulaire ou entre le titulaire et le vérificateur devrait être gérée de manière uniforme, quelle que soit la version du portefeuille utilisée (c'est-à-dire son agent complémentaire).

C'est là qu'un agent numérique entre en jeu. Avec un portefeuille physique, on sait intuitivement comment gérer ses propres justificatifs physiques, il faut les sortir du portefeuille, récupérer le bon justificatif et le présenter adéquatement pour qu’il soit examiné. Une fois délivré, il doit être accepté et placé dans le portefeuille de manière à pouvoir être récupéré en cas de besoin. Avec un portefeuille numérique, ces tâches incombent à l’agent.

Considérez l’agent comme une « enveloppe » logicielle, agissant en votre nom, avec votre portefeuille numérique (le conteneur logiciel). De manière générale, ce logiciel remplit deux fonctions principales:

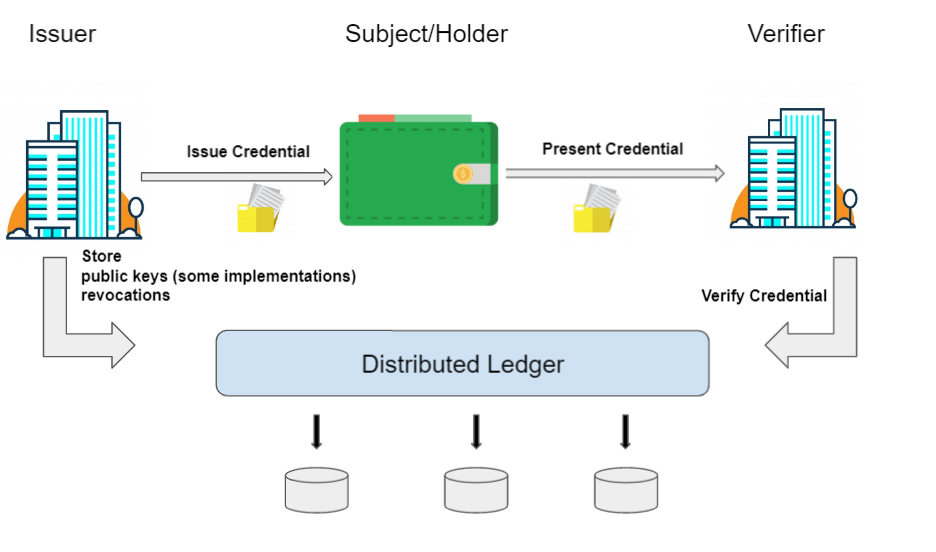
1. Il permet au titulaire de contrôler son justificatif, y compris la gestion du consentement de l'utilisateur, de protéger l'accès logique au portefeuille numérique et de s’assurer que le titulaire, et lui seul, puisse ajouter ou présenter un justificatif;
2. Sur la base de standards, établir et gérer des connexions avec d'autres acteurs pour échanger des justificatifs. Il peut s'agir d'un émetteur ou d'un vérificateur qui tente d'émettre ou de consommer un justificatif;
   * Si l'on se souvient de notre discussion sur la divulgation sélective, la technologie permettant de construire un ensemble d'assertions vérifiables qui répond à la version idéale de l’IAS (c'est-à-dire l'exposition des seules informations granulaires requises à partir de justificatifs multiples) serait un composant de la fonctionnalité de l’agent.

Dans le cadre de l'IAS, plusieurs standards contribuent à définir un comportement cohérent de l’agent. Des standards tels que *Decentralized Identifiers* et plusieurs standards technologiques et standards de protocoles technologiques, qui seront étudiés dans un autre module d'apprentissage, répondent aux exigences de base des logiciels ayant recours aux agents (*agent software*).

### Registre distribué

Le registre distribué est l'endroit où les identifiants décentralisés sont enregistrés afin qu'ils puissent être accessibles à tous. En réalité, il peut s'agir de n'importe quel répertoire d'information. Les propositions de mise en œuvre de l'IAS sont souvent basées sur la technologie de la chaîne de blocs (le *blockchain*). Nous explorerons la technologie de la chaîne de blocs dans un autre module d'apprentissage. Cependant, pour nos besoins ici, les caractéristiques importantes de la chaîne de blocs sont qu'il s'agit d'une base de données distribuée hautement sécurisée qui n'est pas contrôlée par une seule partie.

Voyons comment le registre distribué permet l'IAS. Le schéma ci-dessous illustre l'utilisation d'un registre distribué pour la délivrance et l'utilisation d'un justificatif vérifiable.



Le cycle de vie, de la délivrance à l'utilisation d'un justificatif vérifiable, est le suivant :

* L'émetteur crée un justificatif vérifiable qui est remis au titulaire. Le titulaire et l'émetteur ont établi une relation de confiance et se sont authentifiés mutuellement en utilisant le chiffrement asymétrique et d'autres méthodes de cryptographie à clé publique telles que décrites précédemment..
* L'émetteur stocke les clés nécessaires à la vérification des signatures dans le registre distribué.
* Lorsque le titulaire présente un justificatif au vérificateur, le vérificateur et le titulaire peuvent établir la confiance et sécuriser l'échange d'informations en utilisant des méthodes de cryptographie à clé publique. Lorsque des clés publiques sont requises, le registre distribué est consulté, car tous les acteurs y enregistrent leurs clés publiques.
* Le vérificateur doit ensuite s'assurer que le justificatif n'a pas été falsifié et qu'il est valide. Le registre distribué est consulté pour lire la clé publique de l'émetteur utilisée pour vérifier la signature numérique afin de s'assurer de l'origine et s’assurer que le justificatif n'a pas été altéré depuis sa délivrance. Il est possible, mais pas toujours nécessaire, que le vérificateur consulte le registre distribué pour voir si le justificatif a été révoqué depuis sa création.

### Chaîne de blocs

Tel que mentionné, le registre distribué, considéré comme l'un des principaux fondements de l'IAS, sert de base à la vérification d'un justificatif vérifiable. Bien qu'il puisse s'agir de tout type de stockage disponible dans l'écosystème d'identité numérique, la plupart des modèles proposés utilisent la technologie de la chaîne de blocs comme base du registre distribué.

Dans un module ultérieur, nous étudierons cette technologie de plus près. Dans ce module, nous examinerons ses caractéristiques fonctionnelles et la manière dont elle répond aux exigences de l'IAS en matière de registres distribués.

Tout d'abord, nous devons comprendre un peu ce qu'est une chaîne de blocs. La chaîne de blocs stocke les transactions dans des blocs séquentiels de transactions au fur et à mesure qu'elles se produisent. Les chaînes de blocs sont stockées sur des réseaux distribués de bases de données de chaînes de blocs, toutes des copies les unes des autres appelées des *nœuds*. Lorsqu'un bloc est ajouté, il est répliqué et ajouté à tous les noeuds. Si le réseau de chaînes de blocs l'autorise, lorsqu’un bloc est modifié, la majorité des nœuds du réseau doivent convenir de la validité de la modification. Si un pirate informatique tentait de modifier une transaction, ou d’en ajouter une nouvelle, il devrait apporter le même changement à au moins 51% des nœuds simultanément. Une tâche presque impossible lorsque chacun des nœuds est exploité de manière indépendante. C'est ce qui permet la confiance dans le fait que les données de la chaîne de blocs n'ont pas été altérées.

La deuxième caractéristique fonctionnelle importante est la façon dont la chaîne de blocs peut être utilisée pour protéger la vie privée tout en étant capable de fournir la preuve que les informations reçues par le vérificateur (du titulaire) sont authentiques et proviennent d'un émetteur connu. Pour ce faire, les clés publiques utilisées par l'émetteur pour signer numériquement le justificatif sont stockées sur la chaîne de blocs. Lorsque le vérificateur souhaite examiner un justificatif, il peut récupérer ces clés pour vérifier la signature. Toute modification au justificatif après sa délivrance sera détectée au cours de ce processus.

Il est important de noter que les informations réelles du justificatif ne sont *jamais* stockées sur la chaîne de blocs. Cette caractéristique importante (c'est-à-dire l'immuabilité) de la chaîne de blocs *permet au vérificateur d'être certain que les informations sont celles qui ont été délivrées, à partir d'une source immuable par conception.* La chaîne de blocs permet aussi d'effectuer cette vérification sans introduire la nécessité de consulter directement l'émetteur, ce qui réduit considérablement la complexité de l'écosystème de l'identité. Enfin, puisque les informations des justificatifs sont signées cryptographiquement, le titulaire peut les stocker en dehors de la chaîne de blocs sans aucune perte de confiance dans les informations elles-mêmes, tout en gardant le contrôle sur les personnes avec lesquelles il partage ces informations.

Dans notre module d'apprentissage qui explore en détail certaines des technologies les plus importantes, vous trouverez une discussion plus approfondie sur le fonctionnement de la chaîne de blocs.

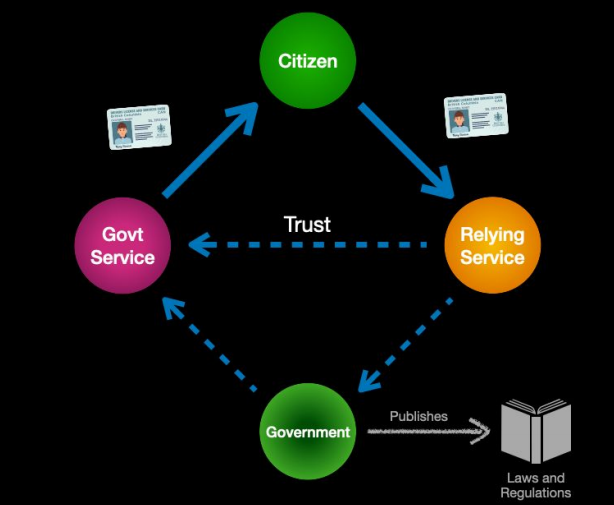
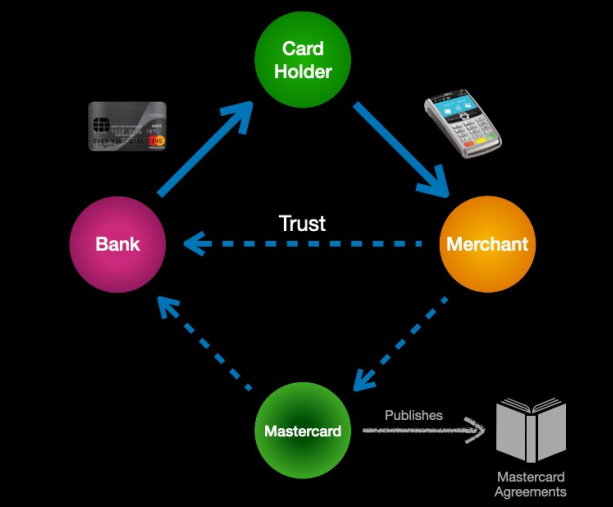
## Trust over IP

### Introduction à Trust over IP

*Trust over IP* (ToIP ou « Confiance dans le protocole Internet ») est une approche globale visant à standardiser la manière dont la confiance en ligne est établie et maintenue. ToIP est dirigée par la [Trust over IP Foundation](https://trustoverip.org/), un projet collaboratif de code source libre sous la tutelle de Linux Foundation.

Plus tôt dans ce module d'apprentissage, nous avons défini le « triangle de la confiance » (c'est-à-dire l'émetteur, le titulaire et le vérificateur) au cœur des justificatifs numériques. Un émetteur qui établit un certain niveau de confiance afin de pouvoir délivrer un justificatif à un titulaire, un titulaire qui choisit de faire suffisamment confiance à un vérificateur pour présenter ce justificatif dans le but de recevoir un service en ligne, et un vérificateur qui choisit de faire confiance à un justificatif délivré par l'émetteur.

La Trust over IP Foundation identifie en outre un « triangle de confiance » en matière de gouvernance. Il s'agit d'une autorité de gouvernance responsable des standards (commerciaux, juridiques et techniques) qui régissent un écosystème d'identité numérique particulier, d'un émetteur qui choisit d'être régi par ces exigences, et de vérificateurs qui choisissent de faire confiance à la solidité du cadre de l'écosystème de l'autorité de gouvernance et à la conformité de l'émetteur à ces standards. Dans leur livre blanc [Introduction to ToIP](https://trustoverip.org/toip-model/), les scénarios d'un service du secteur public et d'un autre du secteur financier sont présentés à titre d'exemple.

[[2]](#footnote-1)

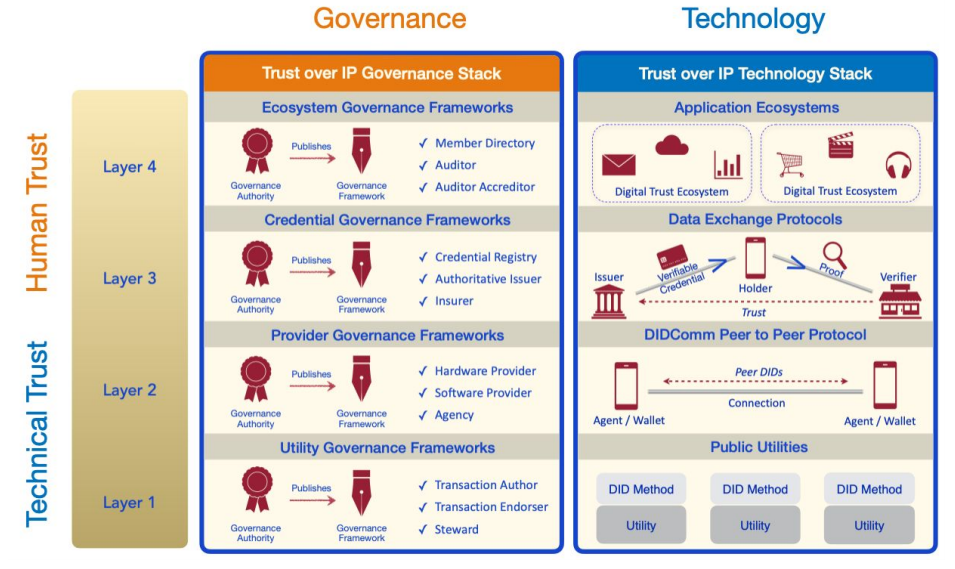
### La pile Trust over IP (Trust over IP Stack)

Comme nous l'avons vu, les modèles centralisés (ou directs) et fédérés (ou du fournisseur d'identité) de justificatifs numériques créent une certaine inefficacité et des défis, lorsqu'ils sont déployés à grande échelle, en particulier si l'on considère la manière dont la confiance est établie dans le monde physique. Dans le monde physique, vous établissez la confiance et un justificatif est délivré (par exemple, votre permis de conduire). Vous le stockez dans votre portefeuille et le présentez à qui vous voulez, lorsque cela est nécessaire. Le modèle pair à pair que nous avons décrit précédemment, ainsi que les avancées dans le monde de l'identité numérique basées sur les justificatifs vérifiables, les identifiants distribués et l’IAS, permettent, pour la première fois, de reproduire cette gestion logique de l'identité dans le monde en ligne. C'est-à-dire que vos émetteurs n'ont pas besoin d'avoir une relation juridique ou contractuelle avec chacun des vérificateurs avec qui vous faites affaire.

Les nombreuses initiatives qui composent ce nouveau modèle de confiance «pair à pair» dans le monde en ligne se sont concentrées sur les nombreux éléments à définir pour rendre un tel écosystème possible. Comme beaucoup d'initiatives dans le monde en ligne, elles se sont concentrées sur l'invention des éléments technologiques, puis sur la manière dont ils s'assemblent sur le plan commercial et sur le plan des processus. *Trust over IP* vise à adopter une approche plus globale en définissant une pile de services complémentaires pour assurer la confiance.

Qu'est-ce qu'une pile? Il s’agit d’un ensemble de services qui s'appuient les uns sur les autres pour créer un écosystème qui fournit un service. Les technologues connaissent la définition de base d'une pile d'un environnement informatique, qui va du matériel sur lequel tout est installé aux réseaux qui assurent l'interconnexion, jusqu'aux applications qui fonctionnent dans l'environnement. Les programmeurs connaissent les piles des langages de programmation qui vont du système d'exploitation aux technologies de stockage des données qu'ils utilisent, en passant par les langages de programmation utilisés pour créer les applications des utilisateurs finaux.

*Trust over IP* propose des pistes complémentaires en matière de technologie et de gouvernance qui abordent les triangles de confiance et de gouvernance tels que décrits ci-dessus. Voici la description qu’en fait la [Trust over IP Foundation](https://trustoverip.org/toip-model/) :

[[3]](#footnote-2)

La pile *Trust over IP*, définie globalement par quatre niveaux dans chacun des composants de gouvernance et technologiques, rassemble les standards que nous avons étudiés dans une vue unifiée qui présente l'ensemble des services nécessaires pour garantir la confiance au sein d'un écosystème d'identité numérique pair à pair.

La pile *Trust over IP* décrite :

| Niveau | Fournit : | Composants de gouvernance : | Composants techniques : |
| --- | --- | --- | --- |
| 1 | Le fondement de la confiance pair à pair, la gestion des identifiants décentralisés et la cryptographie à clé publique qui rendent possible la confiance pair à pair à son niveau le plus bas. | Organe de gouvernance qui spécifie les politiques selon lesquelles les services fournissant des services d’identifiants décentralisés fonctionnent. | Fournit les méthodes d’identifiants décentralisés (notez que celles-ci sont indépendantes de la technologie). |
| 2 | Les standards pour le fonctionnement des composants clés impliqués dans la communication pair à pair. En référence à l'IAS, il s'agit des portefeuilles numériques et des agents qui forment les connexions entre l'émetteur, le titulaire et le vérificateur. | Cadre de gouvernance qui spécifie les standards en matière de protection de la vie privée, de sécurité et de protection des données pour les fournisseurs de portefeuilles et de technologie ayant recours aux agents au sein d'un écosystème. | Les standards technologiques intégrés dans le matériel, les logiciels ou les services  infonuagiques qui fournissent des services de portefeuille et d’agent. |
| 3 | La base pour l'échange de justificatifs et de preuves entre les émetteurs, les titulaires et les vérificateurs. | Le cadre de gouvernance des justificatifs définit qui délivre quels justificatifs, selon quelles politiques, et quel niveau d'assurance. En outre, ce niveau définira les critères pour la délivrance de marques de confiance, le cas échéant, qui permettent aux vérificateurs de prendre leurs décisions de confiance. | Échange de justificatifs, messagerie sécurisée ou automatisation des processus. Les technologies mettant en place l'échange de justificatifs vérifiables en sont un exemple. |
| 4 | Il s'agit des standards qui s'appliquent à l'ensemble des applications de l'écosystème. Les niveaux précédents établissent la «mécanique» nécessaire pour garantir la confiance envers un justificatif vérifiable et ce niveau établit l'ensemble des exigences au plan de l'écosystème qui régissent l'expérience utilisateur cohérente dans l'ensemble de l'écosystème. | L'objectif, les principes et les politiques qui s'appliquent à l'ensemble de l'écosystème. | L'interopérabilité de l'écosystème et les services de confiance non traités autrement dans les niveaux précédents. |

## 

### Vérifiez votre compréhension

Instructions : Dans cette activité, vous devrez choisir entre vrai et faux pour la question associée. Lorsque vous aurez terminé, sélectionnez « Soumettre » en bas de la page.

1. La chaîne de blocs est une exigence absolue de l'IAS. (faux)
2. Les 10 principes de l'identité auto-souveraine constituent une base importante pour le travail actuel sur l'IAS. (vrai)
3. Les fournisseurs d'identité sont des acteurs importants dans tout modèle de l'IAS. (faux)
4. Le W3C est l'organisme de standardisation pour l'IAS. (faux)
5. Les agents des portefeuilles numériques gèrent l'échange de justificatifs dans un modèle d'IAS. (vrai)
6. Les clés publiques sont récupérées à partir du registre distribué dans un modèle d'IAS. (vrai)
7. La sécurité du réseau est la clé de la confiance dans une base de données de chaîne de blocs. (faux)
8. La chaîne de blocs est principalement utilisée pour stocker les informations des justificatifs. (faux)
9. Les nœuds d'une base de données distribuée sont un important concept de la chaîne de blocs et ils sont utilisés pour renforcer la nature immuable des implantations de la chaîne de blocs. (vrai)
10. *Trust over IP* (ToIP) concerne principalement les standards technologiques. (faux)
11. ToIP définit une vue unifiée qui présente l'ensemble des services nécessaires pour assurer la confiance au sein d'un écosystème d'identité numérique pair à pair. (vrai)
12. La ToIP définit des niveaux de gouvernance et technologiques complémentaires qui s'appuient les uns sur les autres. (vrai)

## Entrevues avec des experts

### Entrevue avec Tim Bouma

Nous avons eu l'occasion de parler avec Tim Bouma des façons intéressantes dont les méthodes et les technologies présentées dans ce module d'apprentissage ont permis de repenser nos approches en matière de prestation de services dépendant de l'identité numérique et des justificatifs numériques. Tim est le conseiller principal en identité numérique auprès du dirigeant principal de l'information du gouvernement du Canada.

### Entrevue avec Peter Watkins

Nous sommes heureux d'avoir avec nous Peter Watkins. Peter est le responsable du programme d'identité numérique pancanadienne à l'Institut des services axés sur les citoyens. Peter est un innovateur reconnu dans le domaine de l'identité numérique, avec une vaste expérience en tant que fonctionnaire et agent de changement au sein du gouvernement de la Colombie-Britannique. Peter nous parlera de la divulgation sélective et de la manière dont elle peut permettre une meilleure protection des renseignements personnels.

### Entrevue avec Ian Bailey

Nous avons eu le plaisir de nous asseoir avec M. Ian Bailey, ancien dirigeant principal de l’information de la Colombie-Britannique, pour parler des justificatifs numériques.

## Conclusion

Dans ce module d'apprentissage, nous nous sommes concentrés sur les concepts émergents de conception d'écosystèmes décentralisés liés aux modèles de justificatifs numériques «pair à pair» que nous avons défini dans un module d'apprentissage précédent. Nous avons appris que la conception décentralisée gagne du terrain pour deux raisons principales:

1. Les autres modèles (centralisé et fédéré/ou du fournisseur d'identité) comportent des autorités centrales qui entraînent une certaine inefficacité lorsqu'ils sont déployés à grande échelle. Souvent, ces conceptions d'écosystèmes sont exclusives à l'écosystème lui-même et aux besoins de l'autorité centralisée. Dans de nombreux cas, certaines solutions technologiques exploitées sont souvent basées sur des standards ouverts, mais la conception globale de l'écosystème varie considérablement.
2. La communauté d'identité numérique reconnaît de plus en plus que les modèles pair à pair et décentralisés constituent la prochaine évolution importante des solutions et des écosystèmes de justificatifs numériques. Ce sont ces évolutions majeures qui nous permettront de répondre aux exigences d'une importante législation en matière de protection de la vie privée et des principes clés tels que ceux représentés par la divulgation sélective, de manière automatisée et garantie.

Notre prochain module d'apprentissage s'appuiera sur le contenu présenté ici et traitera de certaines des technologies qui seront nécessaires pour mettre en place des justificatifs numériques centrés sur l'utilisateur tels que décrits dans ce module d'apprentissage.

## Questionnaire du module 6

Vous n'avez qu'un seul essai pour répondre à ce questionnaire de dix-neuf (19) questions sur le module. Ce questionnaire n'est pas chronométré, alors prenez votre temps pour examiner attentivement les options avant de choisir la meilleure réponse.

1. \_\_\_\_\_\_\_\_utilise la même clé pour chiffrer/déchiffrer un message.
   1. \*Le chiffrement symétrique
   2. Le chiffrement asymétrique
   3. Le chiffrement à clé publique
   4. Aucune de ces réponses
2. \_\_\_\_\_\_ utilise une clé pour chiffrer un message et une autre clé mathématiquement liée pour le déchiffrer.
   1. Le chiffrement symétrique
   2. \*Le chiffrement asymétrique
   3. Le chiffrement à clé publique
   4. Aucune de ces réponses
3. La cryptographie à clé publique utilise des méthodes de cryptographie \_\_\_\_\_\_\_\_\_\_\_\_\_.
   1. symétrique
   2. \*asymétrique
   3. RSA
   4. AES
4. La preuve de la délivrance d'un justificatif sans révéler le contenu réel du justificatif est appelée \_\_\_\_\_\_\_\_\_\_\_.
   1. la divulgation sélective
   2. \*la preuve à divulgation nulle de connaissance
   3. un justificatif vérifiable
   4. l’identité auto-souveraine
5. La technologie des registres distribués nécessite une chaîne de blocs pour fonctionner.
   1. Vrai
   2. \*Faux
6. \_\_\_\_\_\_\_\_\_\_\_\_\_ utilise des clés pour faciliter la signature ou le chiffrement des messages.
   1. \*La cryptographie à clé publique
   2. La technologie des registres distribués
   3. Le *Verifiable Credential Data Model*
   4. ToIP
7. Avec l'IAS, les données des justificatifs (ne) sont \_\_\_\_\_\_\_\_\_\_\_ stockées sur le registre distribué afin de s'assurer qu'elles restent infalsifiables.
   1. parfois
   2. toujours
   3. \*jamais
8. \_\_\_\_\_\_\_\_\_\_\_\_ permet(tent) de vérifier que vous savez quelque chose, sans révéler exactement ce que c'est.
   1. La cryptographie à clé publique
   2. Les justificatifs vérifiables
   3. Les identifiants décentralisés
   4. \*Les preuves à divulgation nulle de connaissance
9. La preuve à divulgation nulle de connaissance s'appuie sur la théorie des probabilités pour être statistiquement certain qu'une autre partie possède certaines connaissances précises.
   1. \*Vrai
   2. Faux
10. La possibilité de divulguer de manière sélective des renseignements personnels en fonction des informations dont a réellement besoin un utilisateur final est un élément très important de/du/de la/des \_\_\_\_\_\_\_\_\_\_\_.
    1. \*protection de la vie privée dès la conception
    2. identifiants décentralisés
    3. ToIP
    4. cryptographie à clé publique
11. La chaîne de blocs est une exigence absolue de l'IAS.
    1. Vrai
    2. \*Faux
12. Les 10 principes de l'identité auto-souveraine constituent une base importante pour le travail actuel sur l'IAS.
    1. \*Vrai
    2. Faux
13. Les fournisseurs d'identité sont des acteurs importants dans tout modèle de l'IAS.
    1. Vrai
    2. \*Faux
14. Le W3C est l'organisme de standardisation pour l'IAS.
    1. Vrai
    2. \*Faux
15. Les agents des portefeuilles numériques gèrent l'échange de justificatifs dans un modèle d'IAS.
    1. \*Vrai
    2. Faux
16. Les clés publiques sont souvent récupérées à partir du registre distribué dans un modèle d'IAS
    1. \*Vrai
    2. Faux
17. La sécurité du réseau est la clé de la confiance dans une base de données de chaîne de blocs.
    1. Vrai
    2. \*Faux
18. La chaîne de blocs est principalement utilisée pour stocker les informations des justificatifs.
    1. Vrai
    2. \*Faux
19. La divulgation sélective consiste à envoyer uniquement les données dont le vérificateur a besoin.
    1. \*Vrai
    2. Faux

# Module 7 - Technologies et cadres de référence

## Introduction

Dans une unité d'apprentissage précédente, nous avons examiné certaines des décisions d'architecture qui régissent l'approche adoptée pour mettre en place un service de justificatifs numériques. Nous avons également exploré certaines des approches de conception couramment utilisées qui aident à guider la mise en place d'un modèle d'architecture. Ce module d'apprentissage identifie certaines des technologies et des cadres technologiques les plus répandus qui fournissent une base pour un système ou un service.

L'accent sera mis sur les standards ouverts émergents, les protocoles et les modèles technologiques couramment utilisés dans la mise en place des services de confiance.

Cette liste n'est pas exhaustive. Nous avons identifié quelques-uns des standards, des protocoles et des modèles technologiques les plus importants afin de fournir un point de départ pour la conception de la technologie des solutions pour les justificatifs numériques.

## Objectifs d'apprentissage

* Présenter les standards et les organismes de standardisation.
* Énumérer les technologies d'identité fédérée.
* Nommer les technologies d'identité pair à pair.
* Reconnaître lorsqu'il faut exploiter les technologies émergentes pour assurer une divulgation sélective.

## Standards ouverts

Une grande partie de l'innovation technologique que nous observons aujourd'hui trouve son origine dans les standards ouverts et les logiciels libres. Un logiciel libre est un code source de programmation libre et disponible pour que les gens puissent l'utiliser, le modifier et le partager avec ou sans restrictions. Les standards ouverts sont des standards développés par la communauté qui peuvent être adoptés librement et qui n'enferment pas les utilisateurs dans une implantation propre au fournisseur.

L'Organisation internationale de normalisation ([ISO](https://www.iso.org)) définit une norme comme *un document qui fournit des exigences, des spécifications, des lignes directrices ou des caractéristiques qui peuvent être utilisées de manière uniforme pour s’assurer que le matériel, les produits, les processus et les services sont adaptés à leur objectif* (traduit de l’anglais).

Lorsqu'il s'agit de définir un standard ouvert, il existe plusieurs définitions. Cependant, la plupart des définitions ont en commun les caractéristiques suivantes :

* Développé dans le cadre d'un processus ouvert où toute partie prenante concernée peut contribuer.
* Créé par une collaboration d'experts dans un domaine, et non par une autorité désignée.
* Soumis à un processus de débat et d'évaluation par les pairs ouvert et inclusif.
* Soumis à des processus d'approbation basés sur le consensus de la communauté.
* Ne comporte pas d'exigences qui « attacheraient » délibérément les participants à un fournisseur ou une technologie qui n'est pas en libre accès (par exemple, qui peut être mise en œuvre à l'aide d'un code source libre ou de technologies libres de droits).
* Adhère à des principes qui mettent l'accent sur l'adoption volontaire, en suivant une philosophie d'adoption par le marché basée sur le mérite.

Dans notre définition d'un standard, nous voyons que l'un des principaux objectifs est de favoriser l'uniformité des produits ou des processus qui fournissent un bien ou un service. Les standards ouverts ont également pour objectif principal de réduire les obstacles à l'adoption, en favorisant une adoption à grande échelle (fondée sur le mérite). Cela permet ensuite à une communauté plus diversifiée de participants, petits et grands, de contribuer à la communauté des standards et au développement de technologies innovantes et révolutionnaires basées sur les standards.

## Identité fédérée, les standards technologiques couramment utilisés

**Introduction à la technologie commune**

La plupart des écosystèmes d'identité numérique en production aujourd'hui utilisent les modèles d'écosystèmes d'identité numérique fédérés ou centralisés décrits dans un module d'apprentissage précédent. Les standards technologiques pour la sécurité, le chiffrement et les autres services nécessaires à la protection et à l'échange d'informations d'identité numérique ont évolué jusqu'à ce qu’un certain nombre de technologies habilitantes soient couramment utilisées dans les meilleures pratiques de mise en œuvre des écosystèmes d'identité numérique. Cette section se concentrera sur ces technologies avant de commencer à examiner les technologies plus récentes qui soutiennent les modèles pair à pair et l'identité auto-souveraine.

Les exemples de technologies couramment utilisées pour soutenir plusieurs des modèles de justificatifs numériques centralisés ou fédérés existants comprennent : le langage SAML (*Security Assertion Markup Language*), OAuth, OpenID Connect, les jetons de sécurité (par exemple, les jetons Web simples, les jetons JSON et les assertions du langage SAML) et diverses spécifications des services Web.

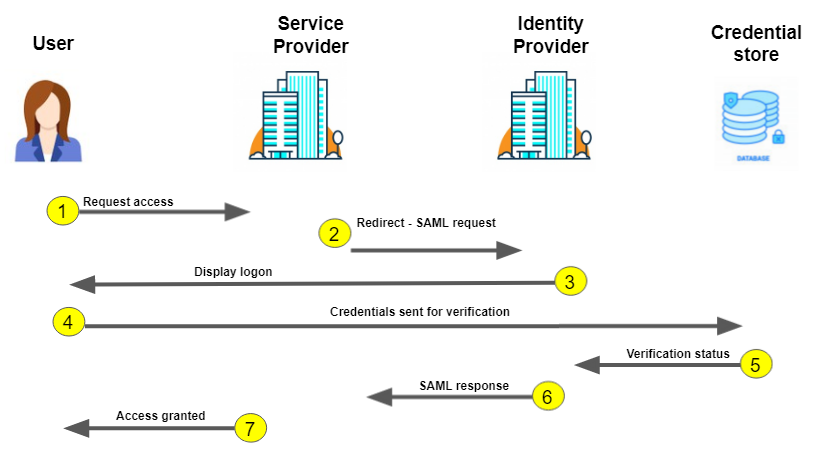
### SAML - Security Assertion Markup Language

SAML (authentification) - [publié par OASIS](http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html)

Le langage SAML (*Security Assertion Markup Language*) est un standard ouvert basé sur le langage XML pour le transfert de données d'identité entre un fournisseur d'identité et l'entité fournissant un service en ligne basé sur l'identité. Cela facilite l'utilisation d'un fournisseur d'identité pour permettre l'accès à plusieurs services en ligne indépendants (identifiés dans le standard comme des fournisseurs de services). L'exemple le plus courant est l'authentification unique mise en place dans la plupart des grandes organisations. Du point de vue de l'identité numérique à travers les organisations, nous voyons cela lors de l'utilisation de justificatifs bancaires ou de médias sociaux pour accéder à d'autres services.

Le langage SAML assure le lien entre l'authentification de l'identité d'un utilisateur et l'autorisation d'utiliser un service. Cette approche fédérée de l'authentification permet d'améliorer le service aux utilisateurs (ceux-ci n'ont pas besoin de conserver des justificatifs d'ouverture de session pour chaque service distinct) et offre un modèle simplifié au fournisseur de services (parfois appelé « utilisateur final »), car dans les faits, il « sous-traite » l'authentification complexe à un fournisseur (c'est-à-dire le fournisseur d'identité) qui dispose d'une fonction d'authentification forte et robuste, souvent avec une base importante de sujets déjà inscrits.

Le langage SAML met en œuvre une méthode sécurisée pour transmettre les authentifications et les autorisations des utilisateurs entre le fournisseur d'identité et les fournisseurs de services. Lorsqu'un utilisateur se connecte à une application compatible au SAML, le fournisseur de services demande une autorisation au fournisseur d'identité approprié. Le fournisseur d'identité vérifie les justificatifs de l'utilisateur, puis renvoie l'autorisation de l'utilisateur au fournisseur de services. L'utilisateur peut alors utiliser l'application. La figure ci-dessous illustre ce processus.



Le langage SAML est une technologie mature et largement utilisée. La version actuelle du standard a été publiée pour la première fois en 2005. Plus récemment, le langage SAML est en concurrence avec certains standards technologiques alternatifs tels que les technologies OAuth et *OpenID Connect* qui s'appuient sur des approches technologiques plus récentes pour fournir des services d'identité fédérée.

### OpenID Connect

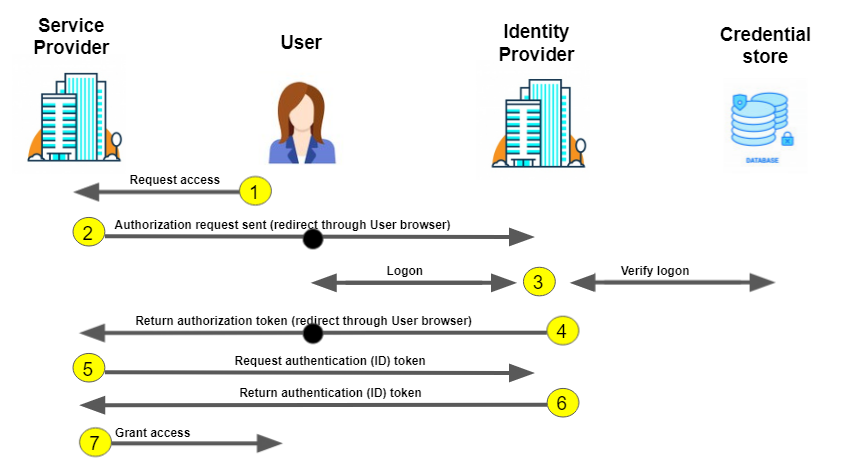
*OpenID Connect* (authentification) - [publié par la fondation OpenID](https://openid.net/connect/)

*OpenID Connect*, publié en 2014, est une évolution des travaux précédents sur *OpenID* reflétés dans des standards remontant à 2006. *OpenID Connect* (OIDC) est un composant d'identité qui s'appuie sur le cadre utilisé pour OAuth, décrit plus loin dans cette section. OIDC, comme le langage SAML, a été conçu pour prendre en charge les interactions d'authentification standardisées entre les fournisseurs de services (identifiés comme «utilisateur final»/«*Relying Party*» dans OIDC) et les fournisseurs d'identité dans un modèle d'identité fédérée.

Si vous avez déjà utilisé vos justificatifs de médias sociaux pour vous authentifier auprès d'un service (par exemple, en utilisant vos informations de connexion de Google ou de Facebook pour accéder à un autre service en dehors des services Google), vous avez certainement utilisé OIDC.

OIDC s'appuie sur le cadre plus efficace qu’est OAuth pour remplacer la nécessité d'interpréter le langage XML (comme c'est le cas avec le langage SAML) par l'utilisation de jetons chiffrés. Cela permet de renforcer la sécurité sur la base de standards et de traiter plus efficacement les informations échangées.

En mettant de côté les complexités d’OAuth et le fonctionnement des jetons pour le moment (nous les explorerons plus en détail dans la section suivante), un modèle générique du fonctionnement d’OIDC est décrit ci-dessous. Il existe plusieurs petites variations de ce modèle que nous ne présenterons pas. Cependant, l'ensemble des interactions de base pour l'authentification par OIDC est représenté.



### OAuth

OAuth (autorisation) - [publié par l’IETF](https://datatracker.ietf.org/doc/html/rfc6749)

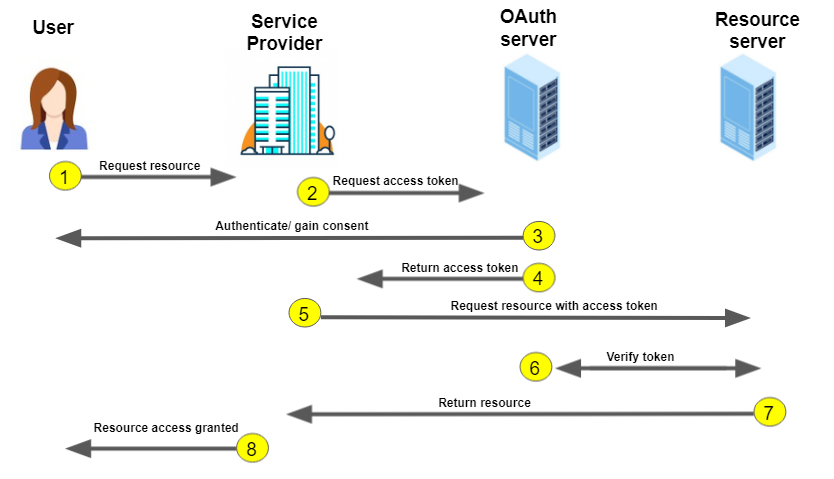
OAuth, publié en 2012, est un standard ouvert de protocole d'autorisation qui permet d'autoriser l'accès à un service. OAuth n'est pas un protocole ou un standard d'*authentification*, c'est un standard d'*autorisation*. Il accorde la permission d'accéder à quelque chose. Il ne fournit pas explicitement d'informations sur l'identité ou le fait qu'une authentification explicite a eu lieu. En substance, OAuth fournit la base d'une interaction sécurisée et standardisée qui demande «Puis-je avoir accès à XXX», et qui répond «Oui, vous pouvez». En supposant que le demandeur et l'organisation qui détient XXX comprennent tous deux OAuth, l'accès à la ressource demandée est accordé.

Utilisé de cette manière, OAuth peut fournir une sorte de pseudo-authentification. Prenons un exemple pour illustrer (*notez que ce que l'utilisateur voit est très près de l'expérience décrite avec OIDC*). Un site Internet vous demande d'utiliser votre compte de média social pour vous connecter à son service - le fournisseur de services formule alors une demande d’autorisation pour accéder au statut d'authentification du média social (le fournisseur d'identité) - cette demande est acheminée par le navigateur de l'utilisateur au le fournisseur d'identité - le fournisseur d'identité confirme l'authentification et renvoie un message d'autorisation, généralement assorti d'un délai de validité. Le fournisseur de services *choisit* alors de considérer ce message comme une confirmation d'authentification. Précédemment, nous avons dit qu’OIDC avait étendu OAuth à des fins d'authentification. Il s'agit essentiellement d'un ajout au processus qui aboutit à la création et à l'échange d'un jeton d'authentification qui confirme qu'une authentification a eu lieu.

Si votre téléphone cellulaire vous a déjà formulé une demande comme «cette application souhaite accéder à votre appareil photo», ou «cette application souhaite accéder à votre compte Google et être autorisée à consulter vos messages électroniques et vos paramètres», vous avez été exposé à OAuth.

La figure ci-dessous illustre le processus général d’OAuth. Il y a quelques éléments à garder à l'esprit en regardant l'illustration :

1. Le standard OAuth intègre le concept de «portée». La portée est la ressource précise à laquelle l'accès est demandé. Dans l'exemple de Google, les «messages électroniques» seraient un exemple de portée.
2. Le consentement est également un composant intégral. Le consentement explicite de l'utilisateur pour accéder à la ressource demandée à partir d'un autre serveur doit être intégré dans les messages échangés avant qu'un jeton d'accès puisse être délivré.
3. Les jetons ont une durée de vie définie, généralement courte, et peuvent faciliter l'accès seulement à la ressource (ou portée) précise demandée.
4. Le jeton d'accès dans l'illustration ci-dessous peut être considéré comme un synonyme du jeton d'autorisation que nous avons mentionné lors de la description d’OIDC.
5. OAuth est utilisé dans plusieurs cas d'utilisation différents. Nous avons fait référence à deux d’entre eux dans cette section. Dans l'exemple des médias sociaux, les messages électroniques de Google sont la ressource à laquelle l'accès est demandé. Dans l'exemple de la «pseudo-authentification», la ressource demandée pourrait simplement être la page du tableau de bord que l'on voit sur une application après s'être connecté.

Comme c'était le cas avec OIDC, il existe quelques variations de processus dans l'utilisation d’OAuth. Nous n'en parlerons pas ici, mais vous trouverez plusieurs sources d'information sur la [page du standard OAuth 2.0](https://oauth.net/2/).

### Jetons Web

Dans la description d’OIDC et d’OAuth, nous avons évoqué l'utilisation de jetons (méta-informations représentant ou faisant référence à quelque chose d'autre) pour permettre l'accès. Avec OIDC, nous voyons deux types de jetons, le jeton d'autorisation ou d'accès, et un jeton d'identité. Il existe de nombreux schémas et standards de jetons, mais pour nos besoins, nous nous intéresserons aux jetons JSON (*JSON Web Tokens* ou JWT) pour comprendre l'utilisation des jetons dans un écosystème d'identité numérique fédérée.

*JSON Web Tokens* (communément prononcé «jot»), [un autre standard de l’IETF](https://datatracker.ietf.org/doc/html/rfc7519), a été publié en 2015. Ce standard définit un conteneur utilisé pour transférer des informations de manière sécurisée. Un jeton JSON est signé numériquement pour prendre en charge la validation de l'origine/l’authenticité, et facultativement chiffré.

Un jeton JSON contient trois composants importants :

1. L'en-tête (*header*) qui identifie la signature et les méthodes de chiffrement utilisées, fournissant les informations nécessaires pour «ouvrir» un jeton JSON.
2. La charge utile (*payload*) qui contient les informations échangées.
3. La signature.

La charge utile contient ce que le standard JWT appelle une assertion. Dans le contexte d'une charge utile d’un jeton JSON, il s'agit d'une ou plusieurs paires de noms/valeurs. Il existe différents types d’assertions.

* Une assertion enregistrée utilise des noms qui sont universellement reconnus. Il existe une dizaine de ces types de noms pour les données couramment utilisées, telles que l'émetteur du jeton JSON, son sujet et son expiration. Par exemple, "iss" nomme l'émetteur (par exemple, la charge utile contiendrait "iss" : "John" comme l'une de ses assertions). Les informations sur le nom de l'assertion (par exemple, "iss") peuvent être répertoriées dans un registre accessible au public afin de fournir un contexte pour comprendre les noms.
* Il peut y avoir des assertions publiques qui utilisent des noms définis uniques dans un certain contexte. Par exemple, un écosystème d'identité numérique spécifique peut définir des noms d'assertions réservés à utiliser dans le contexte des échanges d'informations entre les participants à cet écosystème d'identité numérique. Ces noms définis sont également enregistrés.
* Les assertions privées ou personnalisées peuvent être tout ce que le créateur d'un jeton JSON veut inclure. Ces assertions n'ont pas de composant de registre et l'hypothèse est que le destinataire du jeton JSON comprend le contexte de chacun des noms d'assertion.

Pour créer la partie signature, vous devez prendre l'en-tête codé, la charge utile codée, un secret, l'algorithme indiqué dans l'en-tête, et signer le tout. Ceci est utilisé pour vérifier si le jeton JSON a été modifié en cours de route. Il peut également être utilisé pour vérifier que l'expéditeur est bien celui qu'il prétend être.

Les signatures numériques permettent de garantir l'authenticité du message. Le chiffrement de l'intégralité du jeton JSON le rend illisible pour un tiers pendant la transmission. Si toutes les méthodes de signature ou de chiffrement peuvent être utilisées avec *JSON Web Tokens*, deux autres standards sont plus couramment utilisés: [*JSON Web Signature*](https://datatracker.ietf.org/doc/html/rfc7515) (Signature JSON ou JWS) et [*JSON Web Encryption*](https://datatracker.ietf.org/doc/html/rfc7516) (chiffrement JSON ou JWE). Ce sont deux standards de l’IETF complémentaires qui fournissent un soutien à la signature et au chiffrement pour les jetons JSON.

Pour toute personne souhaitant obtenir plus d'informations sur le jeton JSON, outre les pages de standards dont le lien figure dans cette section, [jwt.io](https://jwt.io/) fournit un ensemble de références plus détaillées.

### Vérifiez votre compréhension

Instructions : Dans cette activité, vous devrez choisir entre vrai et faux pour la question associée. Lorsque vous aurez terminé, sélectionnez « Soumettre » en bas de la page.

1. Les standards ouverts aident les vendeurs de logiciels en faisant la promotion de leurs produits. (faux)
2. Les standards ouverts sont développés et maintenus en collaboration. (vrai)
3. Le langage SAML est un standard d'authentification. (faux)
4. OAuth est un standard d'autorisation (vrai)
5. OAuth s'appuie fortement sur le langage XML pour les messages d'authentification. (faux)
6. OAuth comprend un composant de consentement. (vrai)
7. Le jeton JSON est requis pour que votre système utilise des jetons Web. (faux)
8. Les signatures numériques fournissent une base pour assurer l'authenticité du message d’un jeton JSON. (vrai)
9. Le langage SAML est un standard ouvert pour le transfert de données d'identité. (vrai)
10. OIDC est totalement indépendant d'OAuth. (faux)
11. Les jetons sont une exigence importante des standards d'OAuth et d'OIDC. (vrai)
12. Les signatures JSON sont requises dans un jeton JSON. (faux)

## Modèles de justificatifs numériques pair à pair, les standards technologiques couramment utilisés

Précédemment, nous avons défini les modèles pair à pair comme plaçant le sujet/titulaire d'une identité numérique au centre de l'écosystème, lequel exerce un contrôle direct sur ses justificatifs numériques et la manière dont ils sont partagés. Nous avons approfondi ce sujet en présentant les justificatifs vérifiables et les identifiants décentralisés, ainsi que la manière dont des approches telles que l'identité auto-souveraine (IAS) et la divulgation sélective pourraient fonctionner dans les modèles pair à pair.

Les standards pour ce type de modèle d'écosystème ne sont pas aussi matures que ceux présentés plus tôt dans ce module, mais ils ont gagné en importance au cours des dernières années. Par conséquent, de nombreuses approches technologiques évoluent pour soutenir les modèles pair à pair. En comparaison avec les standards souvent utilisés dans les modèles fédérés, le langage SAML a environ vingt ans et a connu la même évolution décousue, alors que la communauté mettait de l’avant ses meilleures tentatives en matière de standards technologiques et de cadres de référence pour mieux soutenir l'approche, encore nouvelle, des modèles d'identité fédérée. Finalement, les approches basées sur le langage SAML sont devenues de rigueur, utilisées par la plupart. Et ce, jusqu'à ce que de meilleures approches basées sur des standards tels que OIDC et OAuth émergent environ une décennie plus tard. Les travaux actuels sur les écosystèmes d'identité numérique fédérée, nouveaux ou renouvelés, tendent à se concentrer sur ces technologies. Nous pouvons nous attendre à ce que le même processus de consensus communautaire autour des technologies préférées, suivi d'une évolution significative des outils de soutien, se produise dans le domaine pair à pair.

Les sections qui suivent ne sont en aucun cas exhaustives, mais représentent plutôt une tentative visant à mentionner certaines des technologies qui ont commencé à gagner du terrain lors de la mise en œuvre de justificatifs vérifiables et du passage à l'identité auto-souveraine.

## Nous examinerons plusieurs standards technologiques ou cadres de référence différents qui ont été utilisés dans les mises en œuvre de référence de justificatifs vérifiables. Nous nous pencherons principalement sur la manière dont les justificatifs vérifiables sont exprimés, et sur la manière dont ils sont signés et prouvés numériquement.

### JSON and JSON-LD

Le standard *Verifiable Credentials* a publié un [guide d'implantation](https://www.w3.org/TR/vc-imp-guide/#introduction) qui présente des scénarios utilisant JSON et JSON-LD (LD = «*Linked Data*» ou «données liées») comme syntaxe potentielle pour exprimer les données dans un justificatif vérifiable.

JSON est une syntaxe indépendante du langage pour stocker et exprimer des informations. Elle consiste essentiellement en des paires de noms et de données qui ressemblent à ceci lorsqu'on exprime des informations sur un véhicule :

{

make : Chevrolet

model : Corvette

}

[JSON](https://datatracker.ietf.org/doc/html/rfc7159) est largement utilisé dans de nombreux contextes d'application. Il est simple, facile à traiter, utilise un texte lisible par un humain et il est indépendant de la technologie. Il présente toutefois quelques inconvénients. La syntaxe ne transmet pas intrinsèquement de contexte d'information. Cela signifie que le contexte doit être largement compris ou qu'un autre mécanisme doit être créé pour transmettre le contexte. Dans l'exemple ci-dessus, rien ne garantit que le destinataire de ce message comprenne ce que signifient «make» et «model».

[JSON-LD](https://www.w3.org/TR/json-ld11/) a été développé pour fournir ce contexte en étendant la syntaxe JSON de la manière suivante :

{

@context : “http://schema.url/”,

@type : manufacturer

make : Chevrolet

@type : vehicle model

model : Corvette

}

JSON-LD identifie un schéma qui contiendrait le contexte dans lequel s'inscrivent ces données. Dans cet exemple, le schéma présenterait la structure d'information qui indique clairement qu'une structure de niveau supérieur, telle que «véhicule à moteur», peut contenir des informations connexes telles que le fabricant, le nom du modèle, l'année de fabrication, etc. L'information @type fournit des références au schéma d'information global, ce qui signifie que le destinataire peut mieux comprendre «make : Chevrolet» en comprenant qu'il se réfère à l'élément de données «manufacturer» qui fait partie d'un objet d'information plus large décrit dans le schéma et qui se trouve à l'adresse dans le «@context».

Actuellement, JSON-LD semble gagner en popularité en tant que syntaxe plus complète pour exprimer un justificatif vérifiable. Les informations contextuelles permettent au vérificateur de s'assurer qu'il comprend la signification des attributs de données contenus dans un justificatif vérifiable en interprétant simplement le message tout en se référant au schéma identifié qui fournit le contexte complet de tout ce qui pourrait être inclus dans le justificatif.

Voici un exemple simple d’un justificatif vérifiable provenant du *Verifiable Credentials Data Model*, lequel n’a pas encore été traduit à ce jour:

| [EXAMPLE 1](https://www.w3.org/TR/vc-data-model/#example-1-a-simple-example-of-a-verifiable-credential): A simple example of a verifiable credential  {  **// set the context, which establishes the special terms we will be using**  **// such as 'issuer' and 'alumniOf'.**  "@context": [  "https://www.w3.org/2018/credentials/v1",  "https://www.w3.org/2018/credentials/examples/v1"  ],  **// specify the identifier for the credential**  "id": "http://example.edu/credentials/1872",  **// the credential types, which declare what data to expect in the credential**  "type": ["VerifiableCredential", "AlumniCredential"],  **// the entity that issued the credential**  "issuer": "https://example.edu/issuers/565049",  **// when the credential was issued**  "issuanceDate": "2010-01-01T19:73:24Z",  **// claims about the subjects of the credential**  "credentialSubject": {  **// identifier for the only subject of the credential**  "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",  **// assertion about the only subject of the credential**  "alumniOf": {  "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",  "name": [{  "value": "Example University",  "lang": "en"  }, {  "value": "Exemple d'Université",  "lang": "fr"  }]  }  },  **// digital proof that makes the credential tamper-evident**  **// see the NOTE at end of this section for more detail**  "proof": {  **// the cryptographic signature suite that was used to generate the signature**  "type": "RsaSignature2018",  **// the date the signature was created**  "created": "2017-06-18T21:19:10Z",  **// purpose of this proof**  "proofPurpose": "assertionMethod",  **// the identifier of the public key that can verify the signature**  "verificationMethod": "https://example.edu/issuers/keys/1",  **// the digital signature value**  "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5X  sITJX1CxPCT8yAV-TVkIEq\_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN5mgRxD-WUc  X16dUEMGlv50aqzpqh4Qktb3rk-BuQy72IFLOqV0G\_zS245-kronKb78cPN25DGlcTwLtj  PAYuNzVBAh4vGHSrQyHUdBBPM"  }  } |
| --- |

### Conteneurs de justificatifs vérifiables

Maintenant que nous comprenons les options de la syntaxe de base pour exprimer l'information dans un justificatif vérifiable, il y a une deuxième considération syntaxique. Plus précisément, comment les données des justificatifs sont «emballées» de manière à ce que leur authenticité et leur intégrité puissent être vérifiées?

Plus tôt, lorsque nous avons décrit les jetons, nous avons présenté le jeton JSON comme une méthode qui peut être appliquée ici à l'«emballage» d'un justificatif vérifiable. Les données des justificatifs vérifiables, exprimées sous la forme JSON ou JSON-LD, peuvent être présentées sous forme d’un jeton JSON.

En décembre 2020, un projet de spécification proposée pour les [preuves de données liées](https://w3c-ccg.github.io/ld-proofs/) (*Linked Data Proofs* ou *LD-Proofs*) a été publié et définit une autre méthode. Tout comme l'élan ayant donné naissance à la création de JSON-LD, *LD-Proofs* cherche à intégrer un contexte supplémentaire pour aider le destinataire d'une assertion à l'interpréter. En substance, *LD-Proofs* propose une méthode et une syntaxe pour intégrer toutes les informations nécessaires à la vérification des signatures. Pour ce faire, il définit un format JSON-LD standardisé pour l'expression des informations nécessaires au déchiffrement et à la vérification des signatures. Des informations telles que le type de preuve, la méthode de vérification, l'objectif du justificatif et les valeurs de la preuve à interpréter sont rassemblées dans un ensemble standardisé d'informations.

Voici un exemple simple de présentation vérifiable, provenant également du *Verifiable Credentials Data Model*:

| [EXAMPLE 2](https://www.w3.org/TR/vc-data-model/#example-2-a-simple-example-of-a-verifiable-presentation): A simple example of a verifiable presentation  {  "@context": [  "https://www.w3.org/2018/credentials/v1",  "https://www.w3.org/2018/credentials/examples/v1"  ],  "type": "VerifiablePresentation",  **// the verifiable credential issued in the previous example**  "verifiableCredential": [{  "@context": [  "https://www.w3.org/2018/credentials/v1",  "https://www.w3.org/2018/credentials/examples/v1"  ],  "id": "http://example.edu/credentials/1872",  "type": ["VerifiableCredential", "AlumniCredential"],  "issuer": "https://example.edu/issuers/565049",  "issuanceDate": "2010-01-01T19:73:24Z",  "credentialSubject": {  "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",  "alumniOf": {  "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",  "name": [{  "value": "Example University",  "lang": "en"  }, {  "value": "Exemple d'Université",  "lang": "fr"  }]  }  },  "proof": {  "type": "RsaSignature2018",  "created": "2017-06-18T21:19:10Z",  "proofPurpose": "assertionMethod",  "verificationMethod": "https://example.edu/issuers/keys/1",  "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5X  sITJX1CxPCT8yAV-TVkIEq\_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN5mgRxD-WUc  X16dUEMGlv50aqzpqh4Qktb3rk-BuQy72IFLOqV0G\_zS245-kronKb78cPN25DGlcTwLtj  PAYuNzVBAh4vGHSrQyHUdBBPM"  }  }],  **// digital signature by Pat on the presentation**  **// protects against replay attacks**  "proof": {  "type": "RsaSignature2018",  "created": "2018-09-14T21:19:10Z",  "proofPurpose": "authentication",  "verificationMethod": "did:example:ebfeb1f712ebc6f1c276e12ec21#keys-1",  **// 'challenge' and 'domain' protect against replay attacks**  "challenge": "1f44d55f-f161-4938-a659-f8026467f126",  "domain": "4jt78h47fh47",  "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..kTCYt5  XsITJX1CxPCT8yAV-TVIw5WEuts01mq-pQy7UJiN5mgREEMGlv50aqzpqh4Qq\_PbChOMqs  LfRoPsnsgxD-WUcX16dUOqV0G\_zS245-kronKb78cPktb3rk-BuQy72IFLN25DYuNzVBAh  4vGHSrQyHUGlcTwLtjPAnKb78"  }  } |
| --- |

## Chaîne de blocs

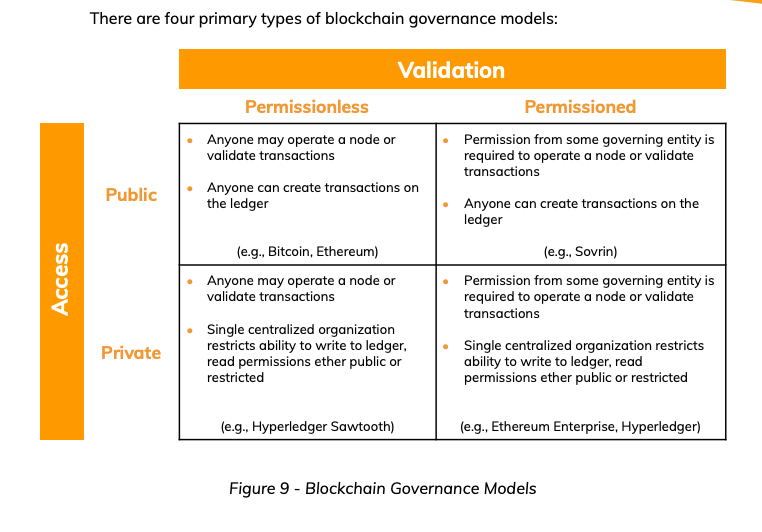
Nous avons précédemment défini la technologie de la chaîne de blocs comme la mise en œuvre commune du registre distribué utilisé dans un écosystème décentralisé. Nous avons dit que cette forme de stockage d'informations peut être rendue largement disponible et qu'elle est immuable, et donc que son intégrité en tant que base de données est intrinsèquement fiable.

Comment cela est-il possible ? Voyons comment fonctionne la chaîne de blocs, puis nous l'appliquerons à son utilisation pour l'identité numérique.

Tout d'abord, nous devons comprendre qu'il existe plusieurs types d'implantation de chaînes de blocs. L'approche de la chaîne de blocs pour les cryptomonnaies (Bitcoin, etc.) est sensiblement différente de celle utilisée pour les justificatifs numériques. Les réseaux de chaînes de blocs peuvent être *sans permission* ou *avec permission*. Dans les implantations sans permission, toute personne disposant de ressources informatiques peut devenir un *nœud* (c'est-à-dire conserver une copie de la base de données de la chaîne de blocs) dans le réseau. Lorsqu'un élément est ajouté à ce type d’implantation, d'importantes ressources informatiques sont utilisées pour trouver une preuve mathématique de la validité d'une transaction ou d'un bloc de transactions. Les mineurs de Bitcoin dont vous avez peut-être entendu parler remplissent cette fonction.

### Implantation de la chaîne de blocs avec permission

La chaîne de blocs, telle qu'elle est mise en place pour les justificatifs numériques, est le plus souvent basée sur une implantation de la chaîne de blocs avec permission. Cela signifie que certaines activités nécessitent une autorisation d'accès. Un réseau est décrit comme fermé lorsque toutes les activités effectuées sur la chaîne de blocs, y compris son accès (lecture) et la possibilité d'ajouter (écriture) à la chaîne de blocs, nécessitent une permission. Comme nous le verrons dans cette section, le modèle utilisé pour la plupart des justificatifs numériques accessibles dans le monde implante un modèle où l'accès (lecture) est ouvert, tandis que la permission de modifier (écriture) la chaîne de blocs est limitée. Par exemple, seul un émetteur de confiance reconnu devrait recevoir l'autorisation, sur la base des principes et procédures de gouvernance du réseau de chaînes de blocs, d'émettre des justificatifs qui seront pris en charge par le réseau. De même, les opérateurs de nœuds de chaînes de blocs doivent être autorisés à exploiter un nœud. Si seuls les émetteurs de confiance peuvent écrire sur la chaîne de blocs, tout le monde peut vérifier. Ce n'est pas si différent de ce que nous connaissons aujourd'hui : seuls les bureaux des véhicules automobiles reconnus peuvent délivrer des permis de conduire valides, mais tout le monde peut les vérifier. L'illustration ci-dessous (*traduite de l’anglais*), de [SOVRIN](http://sovrin.org), présente les types courants d'implantation de chaînes de blocs et des exemples d'utilisation de chacune d'elles.



Dans ce type d'implantation avec permission, il existe différents types de nœuds de chaîne de blocs. Certains nœuds sont simplement là pour fournir des points d'accès pour la lecture des données de la chaîne de blocs. Cela permet de soutenir la large décentralisation de la chaîne de blocs et de répartir la charge de travail de telle sorte qu'aucune copie de la chaîne de blocs ne soit surchargée par le trafic du réseau. Cela permet de se protéger contre les types courants d'attaques telles que le déni de service et offre une évolutivité illimitée pour ce type d'implantation de la chaîne de blocs.

Il existe un plus petit nombre de nœuds qui remplissent la fonction essentielle de vérifier si quelque chose peut être écrit sur la chaîne de blocs. Ils sont souvent appelés des administrateurs (« *stewards* »). Le nombre d'administrateurs est limité, car une forme de consensus doit être atteinte parmi les administrateurs avant que les données ne soient écrites sur la chaîne de blocs. Si le nombre d'administrateurs est trop élevé, ce processus devient inefficace (c'est-à-dire qu'il prend trop de temps et consomme trop de ressources). S'il y en a trop peu, la valeur de plusieurs parties indépendantes acceptant d'enregistrer une transaction est perdue. L'expérimentation avec Hyperledger Indy (nous y reviendrons plus tard) semble indiquer qu'un nombre d’environ 25 administrateurs est optimal.

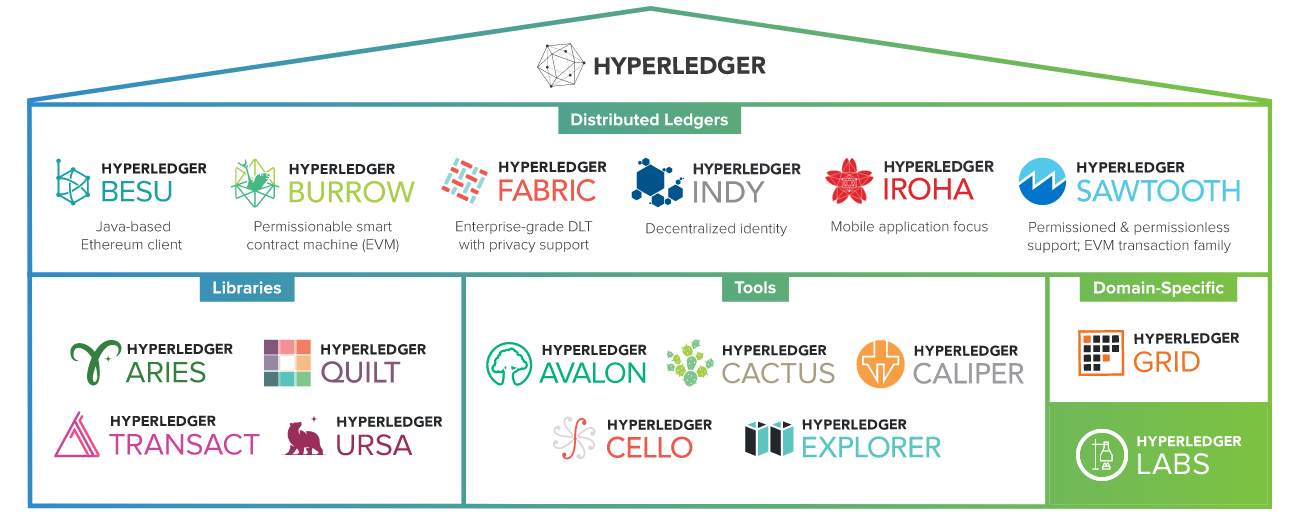
Lorsqu'une transaction doit être inscrite dans le registre, les administrateurs sont chargés de s'assurer qu'elle est valide et peut être enregistrée. Il s'agit notamment de vérifier qu'elle est correctement formée et qu'elle provient d'une source autorisée. Les administrateurs doivent parvenir à un consensus sur la validité de la transaction et son enregistrement dans le bon ordre. L'une des méthodes les plus couramment utilisées s'appelle [*Plenum*](https://hyperledger-indy.readthedocs.io/projects/plenum/en/latest/main.html). Nous n'explorerons pas en détail son fonctionnement interne, mais il suffit de dire qu'un quorum d'administrateurs doit convenir que la transaction est valide et enregistrée dans le bon ordre avant qu'elle ne soit écrite, et que la définition du quorum et la façon dont il est atteint varient selon la méthode de consensus employée.

### Plus d'informations sur la chaîne de blocs

Maintenant que nous avons une idée de la manière dont les données sont stockées sur la chaîne de blocs, comment pouvons-nous dire qu'elles sont immuables? Ceci repose sur une technique appelée le hachage. Le hachage est utilisé pour vérifier si quelque chose a changé. Des algorithmes de cryptographie sont utilisés pour générer une valeur de hachage. La valeur de hachage des données, quelle que soit leur taille, a toujours la même longueur. Le plus populaire à l'heure actuelle est basé sur le SHA256 et génère un hachage de 32 caractères. Un mot introduit dans l'algorithme, ou le contenu d'un roman complet, génère un hachage unique de 32 caractères. Le nombre de valeurs uniques possibles pour ce hachage est d'environ 10, suivi de 77 autres zéros. Cela signifie que le hachage est statistiquement unique. C'est très important, car on peut être sûr que si *un caractère des données d'un bloc change, son hachage sera différent*. Dans le type de réseaux de chaînes de blocs avec permission que nous examinons, le hachage est généré à l'aide d'une technique appelée [*arbre de Merkle*](https://fr.wikipedia.org/wiki/Arbre_de_Merkle). Il s'agit essentiellement d'un hachage interdépendant de telle sorte que la modification d'une transaction entraîne un hachage différent. Lorsque celui-ci est présent dans chaque nœud du réseau, les données compromises (c'est-à-dire les nœuds) peuvent facilement être reconnues et retirées du réseau de la chaîne de blocs jusqu'à ce que le nœud soit resynchronisé avec des données valides. Il est pratiquement impossible que tous les nœuds soient compromis au même moment.

### Hyperledger

L'évolution de la technologie de la chaîne de blocs utilisée dans les solutions de justificatifs numériques est largement contenue dans une série de projets de standards émergents sous l'égide d'[Hyperledger](https://fr.hyperledger.org/), hébergée par Linux Foundation. Les projets hébergés par Hyperledger sont identifiés dans la figure ci-dessous.



Un sous-ensemble de ces projets mérite d'être mentionné, car vous entendrez probablement leurs noms lorsque des implantations de référence de l’identité décentralisée et des approches telles que la divulgation sélective et la preuve à divulgation nulle de connaissance sont décrites.

**NOTE** : il ne s'agit pas d'une liste exhaustive des projets de développement de standards ouverts dans le domaine de la chaîne de blocs pour l'identité numérique, mais simplement d'une liste de quelques-uns des travaux les plus actifs utilisés comme base pour la mise en œuvre de la technologie de la chaîne de blocs pour les justificatifs numériques.

Hyperledger Indy - est au centre de l'écosystème d'identité d'Hyperledger. Il met en œuvre la technologie de base des registres distribués et se compose de deux bibliothèques de code principales. Le nœud indy (*indy-node*) est le composant de la «base de données partagée», ou le registre distribué, de la chaîne de blocs d'Indy. Indy-sdk est un kit de développement logiciel qui permet l'interaction avec le registre distribué et d'autres composants de stockage tels que les portefeuilles numériques. Il s'agit d'une implantation de la chaîne de blocs spécialement conçue pour l'identité numérique, adaptée à la gestion de justificatifs vérifiables et à des modèles d'architecture tels que ceux que nous avons identifiés dans les modules d'apprentissage précédents (pair à pair, triangle de confiance, portefeuilles numériques, etc.).

Hyperledger Aries - fournit un ensemble standardisé de protocoles qui permettent la communication avec le registre distribué et la communication avec un portefeuille numérique. Il s'agit d'une base standard pour les *agents* essentiels que nous avons décrits dans un module d'apprentissage précédent. L'indy-sdk fournit un ensemble uniforme de méthodes pour effectuer des opérations telles que la lecture et l'écriture dans le registre distribué, ou le stockage d'informations dans une mise en œuvre de portefeuille numérique. Cependant, lorsqu'il était question de créer les agents qui interagissent avec le registre et entre eux, il y a eu une prolifération d'implantations spécialement conçues à cet effet qui n'interagissaient généralement pas avec des agents construits par d'autres. Cette situation a conduit à la création d'Aries pour développer les standards qui permettront aux agents d'interagir. Aries se concentre sur les opérations de transmission, de stockage et d'utilisation de justificatifs vérifiables. Certaines des fonctions initiales du projet Indy sont migrées vers Aries.

Hyperledger Ursa - est le résultat de la reconnaissance du fait que les bibliothèques de cryptographie dans Indy devraient vraiment être un projet distinct pour maximiser la réutilisation des capacités cryptographiques et faciliter la maintenance. L'utilisation par d'autres projets, sous l'égide d'Hyperledger ou non, est devenue plus facile. Les éléments cryptographiques du projet Indy ont été transférés d'Indy pour former la bibliothèque initiale d'Ursa.

## Divulgation sélective

### Introduction à la technologie relative à la divulgation sélective

Dans un module d'apprentissage précédent, nous avons défini la divulgation sélective, qui consiste à ne divulguer que ce qui doit l'être pour l’objet recherché. En outre, nous avons présenté le scénario le plus complexe dans lequel un sous-ensemble d'attributs provenant de plusieurs justificatifs était nécessaire pour effectuer une divulgation sélective à un vérificateur.

Les technologies que nous avons présentées jusqu'à présent ne permettent pas à elles seules la divulgation sélective. Afin de préserver la sécurité et l'intégrité nécessaires dans un écosystème d'identité numérique, le vérificateur doit pouvoir être certain de l'origine d'un justificatif et que le titulaire qui présente ces justificatifs est bien celui qu'il prétend être. Les technologies présentées jusqu'à présent supposent que l'ensemble du justificatif est signé par l'émetteur. Dans un scénario de divulgation sélective, il est nécessaire de ne présenter qu'un sous-ensemble du justificatif. Le fait de séparer un justificatif de cette manière invaliderait la signature de l'émetteur et empêcherait le vérificateur de s'assurer systématiquement de l'origine du justificatif.

Pour mettre en œuvre la divulgation sélective, il convient de décrire quelques technologies et méthodes supplémentaires.

### Signatures numériques multimessages

Pour permettre la divulgation sélective, il est nécessaire *que l'émetteur signe chaque élément d'information individuel qui peut être utilisé de manière indépendante*. Pour la divulgation sélective, cela signifie chaque attribut individuel du justificatif. Les systèmes de signature numérique traditionnels reposent sur la signature d'un message dans son intégralité, et non de ses éléments individuels.

Récemment, une spécification appelée [*BBS+ Signatures*](https://w3c-ccg.github.io/ldp-bbs2020/) a été publiée en tant que projet de spécification permettant la signature d'un éventail de messages. Dans le cas d'un justificatif vérifiable, chacun des attributs d'un justificatif délivré peut être signé.

Il existe d'autres méthodes de signature multimessages. Nous avons mis en évidence les signatures BBS+ parce qu'elles intègrent également la cryptographie qui fournit des preuves à divulgation nulle de connaissance au vérificateur. Il s'agit essentiellement de la capacité à analyser un justificatif dans ses composants ET de le présenter de telle sorte que la valeur du justificatif ne soit pas nécessairement transmise, simplement une preuve immuable de sa délivrance.

C'est la pièce manquante pour permettre une divulgation sélective efficace sans compromettre la capacité du vérificateur à s'assurer de l'origine de l'assertion du justificatif. Cette capacité, combinée à la capacité inhérente de la syntaxe JSON-LD de fournir le contexte de l'information, permet l'extraction d'éléments de justificatifs dans une présentation cohérente tout en garantissant que le contexte de chacun des attributs accompagne les données. Ainsi, cela permet au vérificateur d'interpréter l'assertion.

### Exemple de divulgation sélective

Maintenant que nous avons discuté de la plupart des technologies importantes, voyons la divulgation sélective en action.

Par exemple, lorsqu'on nous demande une preuve d'âge, nous fournissons actuellement quelque chose comme un permis de conduire avec notre photo (pour qu'il soit possible de déterminer si le permis appartient au titulaire) et notre date de naissance. Cependant, le vérificateur peut également voir l'adresse du domicile et le reste des informations du justificatif. Des informations qui ne sont pas nécessaires à cette fin. Une divulgation sélective permettrait de ne montrer que les deux informations nécessaires au vérificateur.

Passons en revue la délivrance et l'utilisation d'un justificatif vérifiable qui se prête à une divulgation sélective. Comme indiqué précédemment, de nombreuses méthodes technologiques ont été expérimentées pour permettre la divulgation sélective. Pour les besoins de notre exemple, nous supposerons l'utilisation de [JSON-LD](https://www.w3.org/TR/json-ld11/) avec des [signatures BBS+](https://w3c-ccg.github.io/ldp-bbs2020/), car cette approche semble être de plus en plus considérée comme la meilleure option pour parvenir à une divulgation sélective, avec l'avantage supplémentaire de mettre en œuvre une preuve à divulgation nulle de connaissance.

1. Création et délivrance :

L'émetteur suivra son processus commercial et décidera de délivrer un justificatif. Ce justificatif utilisera le *Verifiable Credentials Data Model* du W3C pour construire notre justificatif. L'utilisation de JSON-LD fournira une syntaxe améliorée qui intégrera le contexte avec les informations dans le justificatif délivré.

L'étape suivante consiste à signer numériquement le justificatif créé. C'est là qu'intervient la première exigence importante. La méthode de signature doit permettre une divulgation sélective. La méthode des signatures BBS+ est l'une de ces méthodes qui nous permettent de *signer plusieurs messages*. Les signatures multimessages permettent l’analyse syntaxique en aval d'un justificatif de sorte que seuls les attributs d'identité requis soient exposés à un vérificateur. Un schéma de signature à messages multiples est nécessaire pour la délivrance de justificatifs. Si le justificatif n'est pas signé d'une manière qui prend en charge la divulgation sélective, il importe peu que le portefeuille numérique du titulaire puisse construire une assertion de divulgation sélective ou que le vérificateur puisse interpréter une assertion de divulgation sélective.

Bien entendu, les clés publiques utilisées pour la signature doivent être rendues disponibles. L'approche la plus populaire consiste à utiliser des identifiants décentralisés, tels que définis dans le standard *Decentralized Identifiers* en cours de développement au W3C. Les identifiants décentralisés créés peuvent être stockés soit dans le registre distribué (s'ils doivent être largement disponibles), soit avec le titulaire (s'ils ne sont nécessaires que pour un échange de justificatifs précis).

Pendant la construction du justificatif, l'émetteur utilisera une clé publique mise à disposition par le titulaire pour lier inextricablement le justificatif au titulaire et permettre de prouver en aval la fiabilité du processus de délivrance. Dans notre exemple, chacun des attributs du justificatif est ensuite signé numériquement à l'aide des signatures BBS+. L'utilisation de JSON-LD et de ses informations contextuelles intégrées nous aide à comprendre que cet ensemble d'assertions signées individuellement peut être combiné en une structure de plus haut niveau, dans ce cas, un permis de conduire.

Le justificatif est alors délivré au titulaire, qui le place dans son portefeuille. Il y a une autre hypothèse implicite ici, à savoir que l'émetteur et la technologie du portefeuille du titulaire comprennent tous deux les méthodes sécurisées pour cette connexion et ce transfert du justificatif vérifiable. Il existe plusieurs méthodes pour y parvenir que nous n'aborderons pas dans ce programme d'apprentissage.

1. Présentation et utilisation du justificatif vérifiable :

Notre titulaire dispose désormais d'un justificatif vérifiable prêt pour la divulgation sélective dans son portefeuille numérique.

Le vérificateur doit informer le titulaire des informations qui sont requises. Un effort de développement collaboratif communautaire est en cours pour mettre au point un ensemble standardisé de méthodes pour échanger une présentation de justificatifs vérifiables, dont la première étape consiste à formuler et à comprendre une demande d'informations. Vous pouvez baser ce travail sur un protocole d'échange de présentation de justificatifs vérifiables ([*Presentation Exchange*](https://identity.foundation/presentation-exchange/)) entrepris à la Decentralized Identity Foundation([DIF](https://identity.foundation/)).

Le portefeuille du titulaire assemble ensuite une assertion à partir d'un sous-ensemble d'attributs signés reçus de l'émetteur, et signe numériquement l'ensemble de l'assertion. Cette présentation d'une assertion vérifiable est remise au vérificateur. Pour nos besoins, nous supposerons que la méthode utilisée ici est une méthode sécurisée qui préserve la confiance dans l'intégrité de l'échange.

Le vérificateur dispose maintenant d'une assertion vérifiable consistant en un message (ou une présentation d'assertion, signée par le titulaire) qui contient des assertions individuelles signées par l'émetteur. Le vérificateur, en utilisant les clés publiques stockées sur le registre distribué, peut maintenant vérifier la ou les signatures du titulaire pour s'assurer que le message a bien été envoyée par le titulaire avec lequel il pense traiter, et utiliser les clés publiques de l'émetteur pour s'assurer que le justificatif provient de l'émetteur attendu.

En outre, l'utilisation de JSON-LD avec les signatures BBS+ permet à la présentation des justificatifs vérifiables de ne fournir que les informations requises pour une preuve à divulgation nulle de connaissance, et non les valeurs des données d'attributs d'identité.

Ce cas d'utilisation a été présenté à un niveau relativement élevé. Une étude approfondie sera nécessaire pour comprendre pleinement les subtilités de son fonctionnement aux niveaux technologiques les plus bas. Les standards requis sont disponibles en suivant les liens dans ce module d'apprentissage. En outre, les deux ressources suivantes ont été des références utiles lors de la rédaction de certaines parties de ce module d'apprentissage:

Le document [Verifiable Credentials explained](https://www.lfph.io/wp-content/uploads/2021/02/Verifiable-Credentials-Flavors-Explained.pdf), publié par [Covid-19 Credentials Initiative](https://www.covidcreds.org/) et une [courte explication simplifiée de la divulgation sélective et de la signature multimessages](https://learn.mattr.global/concepts/selective-disclosure) publiée par [MATTR](https://learn.mattr.global/).

### Vérifiez votre compréhension

Instructions : Dans cette activité, vous devrez choisir entre vrai et faux pour la question associée. Lorsque vous aurez terminé, sélectionnez « Soumettre » en bas de la page.

1. Les standards de données liées sont utilisés pour lier les justificatifs de différents émetteurs. (faux)
2. JSON-LD étend la syntaxe JSON pour fournir un contexte d'information. (vrai)
3. Un jeton JSON, contenant un justificatif vérifiable, doit utiliser JSON-LD. (faux)
4. La technologie de la chaîne de blocs pour l'identité numérique est généralement différente de celle utilisée pour la cryptomonnaie. (vrai)
5. Les signatures BBS+ sont un composant obligatoire de la divulgation sélective. (faux)
6. Les valeurs de hachage sont utilisées pour fournir une liaison séquentielle des blocs de données dans une base de données de chaîne de blocs. (vrai)
7. Les standards pour les modèles d'écosystèmes d'identité numérique pair à pair ne sont pas encore matures et largement adoptés. (vrai)
8. La spécification proposée pour les preuves de données liées (*LD-Proofs*) vise à intégrer toutes les informations nécessaires à la vérification des signatures. (vrai)
9. Les preuves de données liées (*LD-Proofs*) remplacent le besoin de JSON-LD. (faux)
10. Les identifiants décentralisés sont des conteneurs primaires pour les informations de justificatifs. (faux)
11. Des signatures multimessages d'un certain type sont nécessaires pour mettre en place un système de divulgation sélective. (vrai)

## Entrevue avec des experts

### Entrevue avec Kaliya Young (Identity Woman)

Kaliya Young, célèbre ambassadrice de l'évolution dans le monde de l'identité numérique, nous offre un aperçu supplémentaire du changement radical que certaines de ces technologies peuvent représenter pour nous. Kaliya est une experte en identité auto-souveraine et en identité sur la chaîne de blocs. Elle est co-auteur d'un guide complet sur l'identité auto-souveraine, et co-fondatrice de l’Internet Identity Workshop.

<<Kaliya Young interview goes here>>

### Entrevue avec John Jordan

Nous avons eu l'occasion de nous entretenir avec John Jordan, directeur général du service de confiance numérique de la Colombie-Britannique (le BC Digital Trust Service). M. Jordan a été à l'avant-garde de l'innovation dans la prestation de services dépendant de justificatifs numériques. Nous discutons avec John de certaines des technologies émergentes dans le domaine des justificatifs numériques et de la façon dont le secteur public au Canada peut se positionner pour tirer parti de ces importantes avancées.

## Conclusion

Ce module d'apprentissage a décrit certaines des technologies couramment utilisées pour mettre en œuvre des justificatifs numériques basés sur des standards. Cependant, comme nous l'avons noté à plusieurs reprises, il existe de nombreux standards émergents développés ou en cours de développement. Nous avons tenté de recenser et de décrire ceux qui nous semblent les plus importants. Cependant, si votre quête d'apprentissage a pour but de devenir un expert en matière de justificatifs numériques, vous devriez considérer ce matériel comme un bon point de départ dans votre cheminement et étudier le matériel plus détaillé mentionné dans ce programme d'apprentissage.

Dans ce module d'apprentissage, nous avons mentionné certains des standards ouverts les plus couramment utilisés et intégrés dans les systèmes utilisés pour fournir des modèles de justificatifs fédérés. De même, nous avons indiqué quelques-uns des standards ouverts et des technologies émergentes les plus importants pour les modèles pair à pair et les justificatifs vérifiables.

Comme indiqué dans ce module d'apprentissage, les approches fédérées des justificatifs numériques sont les modèles les plus répandus qui sont actuellement en place et fonctionnent. Cependant, les approches pair à pair en cours de développement gagnent en popularité et semblent être la prochaine étape dans l'évolution des justificatifs numériques, une évolution qui met systématiquement en œuvre les principes de protection de la vie privée décrits dans les modules précédents de ce programme d'apprentissage.

## Questionnaire du module 7

Vous n'avez qu'un seul essai pour répondre à ce questionnaire de vingt (20) questions sur le module. Ce questionnaire n'est pas chronométré, alors prenez votre temps pour examiner attentivement les options avant de choisir la meilleure réponse.

1. *OpenID Connect* est un standard d’/de \_\_\_\_\_\_\_\_\_\_\_ (interopérabilité, autorisation, **authentification**, chiffrement).
2. Le hachage cryptographique est susceptible de faire l'objet de rétro-ingénierie et il faut s'en prémunir. (Vrai, **Faux**)
3. L'un des premiers standards ouverts basés sur le langage XML largement adopté pour le transfert de données d'identité entre un fournisseur d'identité et l'entité fournissant le service en ligne s'appelait \_\_\_\_\_\_\_\_\_\_\_. (XACML, SGML, **le langage SAML**, IDXML)
4. Les standards *Linked Data* (données liées) étendent les standards technologiques existants afin de fournir \_\_\_\_\_\_\_\_\_\_ pour les données échangées. (une meilleure sécurité, une interopérabilité renforcée, **du contexte**, d’autres méthodes)
5. Le vérificateur d'un justificatif vérifiable doit consulter l'émetteur du justificatif pour s'assurer que le justificatif est valide. (Vrai, **Faux**)
6. Oauth est un standard d’/de \_\_\_\_\_\_\_\_\_\_\_ (interopérabilité, **autorisation**, authentification, chiffrement).
7. L'une des exigences technologiques fondamentales pour la mise en œuvre de la divulgation sélective est (choisissez la MEILLEURE) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. (le jeton JSON, Oauth, **la signature multimessages**, la chaîne de blocs)
8. *OpenID Connect* s'appuie sur les approches Oauth pour l'échange de messages. (**Vrai**, Faux)
9. Oauth traite les messages XML plus rapidement. (Vrai, **Faux**)
10. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ est/sont un effort de développement communautaire collaboratif en cours pour mettre au point un ensemble standardisé de méthodes permettant d'échanger une assertion de justificatif vérifiable d'une manière qui soutient la divulgation sélective. (JSON-LD, Les signatures BBS+, **L’échange de présentation (*Presentation Exchange*)**, La preuve à divulgation nulle de connaissance)
11. La preuve de divulgation nulle de connaissance est un composant clé de la divulgation sélective. (Vrai, **Faux**)
12. L'une des principales fonctions d'un document d'identifiant décentralisé (*DID document*) est de stocker les \_\_\_\_\_\_\_\_\_\_ nécessaires à la vérification des justificatifs. (clés privées, attributs des justificatifs, assertions du langage SAML, **clés publiques**, données liées).
13. Le registre distribué est utilisé pour stocker en toute sécurité les données des justificatifs vérifiables. (Vrai, **Faux**)
14. Dans un schéma de justificatif vérifiable, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ permet/permettent la vérification d'un justificatif sans avoir à consulter directement l'émetteur. (les données liées, **le** **registre distribué**, JSON-LD, la signature multimessage, les jetons JSON)
15. Le jeton JSON est un exemple de \_\_\_\_\_\_\_\_\_\_\_\_\_\_. (justificatif, méthode de signature numérique, standard d'échange de messages, **jeton de sécurité**)
16. JWT, JWE et JWS sont des standards publiés par l’/le\_\_\_\_\_\_\_\_\_\_\_\_\_. (**IETF**, ISO, OASIS, W3C)
17. \_\_\_\_\_\_\_\_\_\_ comprend/incluent les concepts d'inclusion du consentement explicite pour accéder à une ressource dans l'échange de messages. (Le langage SAML, **Oauth**, Les signatures BBS+, Les jetons JSON)
18. \_\_\_\_\_\_\_\_\_\_\_\_\_ est/sont un composant d'identité qui s'appuie sur le cadre utilisé pour OAuth
    1. Le langage SAML (*Security Assertion Markup Language*)
    2. OAuth
    3. \**OpenID Connect* (OIDC)
    4. Les jetons de sécurité
19. Pour permettre la divulgation sélective, il est nécessaire que l'émetteur signe chaque élément d'information individuel qui peut être utilisé de manière indépendante.
    1. \*Vrai
    2. Faux
20. La chaîne de blocs, telle qu'elle est mise en place pour les justificatifs numériques, est le plus souvent basée sur une implantation de la chaîne de blocs sans permission.
    1. Vrai
    2. \*Faux
21. \_\_\_\_\_\_\_est/sont utilisé(e)(s) pour vérifier si quelque chose a changé.
    1. JSON
    2. Les preuves de données liées (*LD-Proofs)*
    3. La chaîne de blocs
    4. \*Le hachage

## Post-évaluation

Merci d’avoir participé au projet pilote sur les approches éducatives.

Nous espérons que vous avez apprécié le programme et que vous en avez appris davantage sur les justificatifs numériques!

Afin d'assurer un suivi, nous aimerions vous poser quelques questions sur votre expérience. Les informations recueillies seront utilisées pour évaluer le programme et nous aider à apporter des améliorations pour la prochaine version. Il y a 32 questions au total, et nous estimons qu'il vous faudra environ 15 à 20 minutes pour y répondre.

Conditions d'utilisation

Merci encore pour votre participation, vos commentaires sont précieux.

*L'équipe d'Innovation, science et développement économique (ISDE)*

*Digital Identity Lab / Laboratoire d'identité numérique*

>>1. Un mot de passe est un exemple de/d’\_\_\_\_\_\_\_\_\_\_\_\_\_. <<

( ) justificatif

( ) vérificateur

(x) authentifiant

( ) attribut d'identité

>>2. \_\_\_\_\_\_\_\_\_ confirme l'exactitude des informations présentées, tandis que \_\_\_\_\_\_\_\_\_ assure qu'elles appartiennent à l'entité à laquelle s'applique l'assertion d'identité. <<

(x) La validation, la vérification

( ) L’authentification, la validation

( ) L’authentification, la vérification

( ) La vérification, la validation

>>3. Une preuve \_\_\_\_\_\_\_\_\_\_\_ en matière de justificatifs ne s'applique qu'à une personne ou une organisation légalement reconnaissable. <<

( ) numérique

(x) fondamentale

( ) contextuelle

( ) authentique

>>4. Votre justificatif peut être utilisé pour accéder à quelque chose (par exemple, un service en ligne) <<

( ) Vrai

(x) Faux

>>5. \_\_\_\_\_\_\_\_\_\_\_\_ est le processus qui consiste à établir que le sujet du justificatif numérique peut être décrit de manière à être unique dans l'ensemble des justificatifs numériques délivrés. <<

( ) La validation

( ) La vérification

( ) L’authentification

(x) La résolution

>>6. Le gouvernement fédéral a formellement défini \_\_ niveaux d'assurance (NdA) pour les justificatifs numériques. <<

( ) 2

(x) 4

( ) 6

( ) 8

>>7. La/Les \_\_\_\_\_\_\_\_\_ définit/définissent la façon dont le gouvernement fédéral doit traiter les renseignements personnels. <<

(x) *Loi sur la protection des renseignements personnels*

( ) LPRPDE

( ) PIPA

( ) lois provinciales sur la protection des renseignements personnels

>>8. Les \_\_\_\_\_\_\_\_\_\_\_\_ expriment les objectifs et les intentions d'une organisation, tandis que les \_\_\_\_\_\_\_\_\_\_\_\_ définissent formellement ce qui sera fait et comment. <<

( ) règlements, standards

( ) standards, politiques

( ) procédures, règlements

(x) politiques, procédures

>>9. « Les menaces à la vie privée devraient être anticipées et prévenues avant qu'elles ne se produisent » fait partie \_\_\_\_\_\_\_\_\_\_. <<

( ) de la LPRPDE

( ) des 10 principes relatifs à l'équité dans le traitement de l'information

(x) de la protection de la vie privée dès la conception

( ) de la *Loi sur la protection des renseignements personnels*

>>10. La capacité de démontrer que les processus de traitement des renseignements personnels sont conformes au niveau d'assurance (NdA) attendu est un élément à prendre en considération lors de l'évaluation de la/de l’\_\_\_\_\_\_\_\_\_\_. <<

( ) protection de la vie privée

( ) convivialité

( ) interopérabilité

(x) responsabilité

>>11. La clé d'un écosystème de justificatifs numériques viable est la/le \_\_\_\_\_\_\_\_\_\_. <<

( ) fiabilité

( ) respect des standards

(x) confiance

( ) convivialité

>>12. La/Le \_\_\_\_\_\_\_\_\_ crée un cadre pour la confiance et l'interopérabilité des justificatifs numériques au Canada. <<

( ) Directive sur la gestion de l'identité

( ) Conseil canadien des normes

(x) Cadre de confiance pancanadien (CCP)

( ) W3C

>>13. Les deux standards souvent cités lors de l'étude des justificatifs vérifiables et de l'identité décentralisée sont le standard *data model for verifiable credentials* et le standard *specification for decentralized identifiers* publiés par le/l’ \_\_\_\_\_\_\_. <<

( ) ISO

(x) W3C

( ) NIST

( ) IETF

( ) CCIAN

>>14. Les modèles d'identité fédérée permettent aux utilisateurs de mieux contrôler leurs renseignements personnels. <<

( ) Vrai

(x) Faux

>>15. Les fournisseurs d'identité de confiance sont la clé des justificatifs vérifiables tels que décrits dans les standards du W3C. <<

( ) Vrai

(x) Faux

>>16. La preuve de la délivrance d'un justificatif sans en révéler le contenu réel est appelée \_\_\_\_\_\_\_\_\_\_\_. <<

( ) la divulgation sélective

(x) la preuve à divulgation nulle de connaissance

( ) un justificatif vérifiable

( ) l’identité auto-souveraine

>>17. Le « triangle de la confiance », souvent utilisé pour décrire les justificatifs numériques, comprend \_\_\_\_\_\_\_\_, le titulaire et le vérificateur. <<

(x) l’émetteur

( ) le sujet

( ) le fournisseur d'identité

( ) le fournisseur de services

>>18. Les standards *Linked Data* (données liées) étendent les standards technologiques existants afin de fournir \_\_\_\_\_\_\_\_\_\_ pour les données échangées. <<

( ) une meilleure sécurité

( ) une interopérabilité renforcée

(x) du contexte

( ) d’autres méthodes

>>19. Le vérificateur d'un justificatif vérifiable doit consulter l'émetteur d'un justificatif pour s'assurer que le justificatif est valide. <<

( ) Vrai

(x) Faux

>>20. Les informations des justificatifs ne sont jamais stockées dans le registre distribué dans le modèle de l’IAS. <<

(x) Vrai

( ) Faux

>>21. Les justificatifs vérifiables sont faciles à manipuler, et il faut s'en prémunir. <<

( ) Vrai

(x) Faux

>>22. Avec les justificatifs vérifiables, un changement d'information nécessite la révocation et la délivrance d'un nouveau justificatif. <<

(x) Vrai

( ) Faux

>>23. Dans les modèles de justificatifs numériques pair à pair ou décentralisés, le titulaire d'un justificatif numérique est toujours le sujet du justificatif numérique. <<

( ) Vrai

(x) Faux

>>24a. Sur une échelle de 1 à 5, en considérant ce que vous savez maintenant, comment évaluez-vous la capacité de votre organisation pour la mise en œuvre d'un système dépendant des justificatifs numériques? Évaluez et tapez votre réponse dans l'espace prévu à cet effet. <<

( ) 1 (faible)

( ) 2

( ) 3

( ) 4

( ) 5 (très élevée)

( ) S. O. - Je ne suis pas sûr(e)

>>24b. Quelles sont les lacunes que vous percevez / de quoi votre organisation aurait-elle besoin pour atteindre ces objectifs? <<

= réponse

>>25a. Sur une échelle de 1 à 5, en considérant ce que vous savez maintenant, comment évaluez-vous la capacité de votre organisation pour la mise en œuvre d'un système dépendant des justificatifs numériques et basé sur des technologies émergentes telles que les portefeuilles numériques et la chaîne de blocs (*blockchain*)? <<

( ) 1 (faible)

( ) 2

( ) 3

( ) 4

( ) 5 (très élevée)

( ) S. O. - Je ne suis pas sûr(e)

>>25b. Quelles sont les lacunes que vous percevez / de quoi votre organisation aurait-elle besoin pour atteindre ces objectifs? <<

>>26. Sur une échelle de 1 à 5, quel est votre degré de confiance dans votre connaissance des lois, règlements et politiques applicables aux justificatifs numériques? <<

( ) 1 (faible)

( ) 2

( ) 3

( ) 4

( ) 5 (très élevé)

( ) S. O. - Je ne suis pas sûr(e)

>>27a. Sur une échelle de 1 à 5, comment évaluez-vous votre niveau de confiance dans les justificatifs numériques? <<

( ) 1 (faible)

( ) 2

( ) 3

( ) 4

( ) 5 (très élevé)

( ) S. O. - Je ne suis pas sûr(e)

>>27b. Quelles sont les lacunes que vous percevez / quelles sont vos préoccupations concernant les justificatifs numériques? <<

>>28a. Sur une échelle de 1 à 5, comment évalueriez-vous votre intérêt ou celui de votre organisation à adopter des justificatifs numériques? <<

( ) 1 (faible)

( ) 2

( ) 3

( ) 4

( ) 5 (très élevé)

( ) S. O. - Je ne suis pas sûr(e)

>>28b. Quelles sont les lacunes que vous percevez / de quoi auriez-vous besoin, vous ou votre organisation, pour atteindre ces objectifs? <<

>>29a. Sur une échelle de 1 à 5, comment évaluez-vous votre expérience dans le cadre de cette formation ?<<

( ) 1 (peu satisfaisante)

( ) 2

( ) 3

( ) 4

( ) 5 (très bonne)

( ) S. O. - Je ne suis pas sûr(e).

>>29b. Y a-t-il une partie du programme que vous avez vraiment appréciée? Veuillez fournir des détails : <<

>>29c. Y a-t-il une partie du programme que vous n'avez pas appréciée? Veuillez fournir des détails : <<

>>30a. Avez-vous obtenu les informations dont vous aviez besoin sur les justificatifs numériques ?<<

( ) 1 (pas du tout)

( ) 2

( ) 3 (quelques-unes)

( ) 4

( ) 5 (toutes)

( ) S. O. - Je ne suis pas sûr(e).

>>30b. Pourquoi ou pourquoi pas? <<

>>31a. Sur une échelle de 1 à 5, dans quelle mesure avez-vous trouvé le matériel facile à comprendre ? <<

( ) 1 (c'était très difficile)

( ) 2

( ) 3 (assez difficile)

( ) 4

( ) 5 (c'était très facile)

>>31b. Pourquoi? <<

>>32a. Quelle est la probabilité que vous recommandiez cette formation à un ami ou à un collègue ?

( ) 1 (faible)

( ) 2

( ) 3

( ) 4

( ) 5 (très élevée)

( ) S. O. - Je ne suis pas sûr(e).

>>32b. Pourquoi ou pourquoi pas? <<

1. Matt McKinney, «*Understand Verifiable Credentials in 10 Minutes*», <https://www.arcblock.io/blog/en/post/2020/04/15/verifiable-credentials> [↑](#footnote-ref-0)
2. *ToIP Foundation*, «*Introducing the Trust over IP Foundation»*, <https://trustoverip.org/wp-content/uploads/sites/98/2020/05/toip_introduction_050520.pdf> [↑](#footnote-ref-1)
3. *ToIP Foundation*, «*Introducing the Trust over IP Foundation*», <https://trustoverip.org/wp-content/uploads/sites/98/2020/05/toip_introduction_050520.pdf> [↑](#footnote-ref-2)