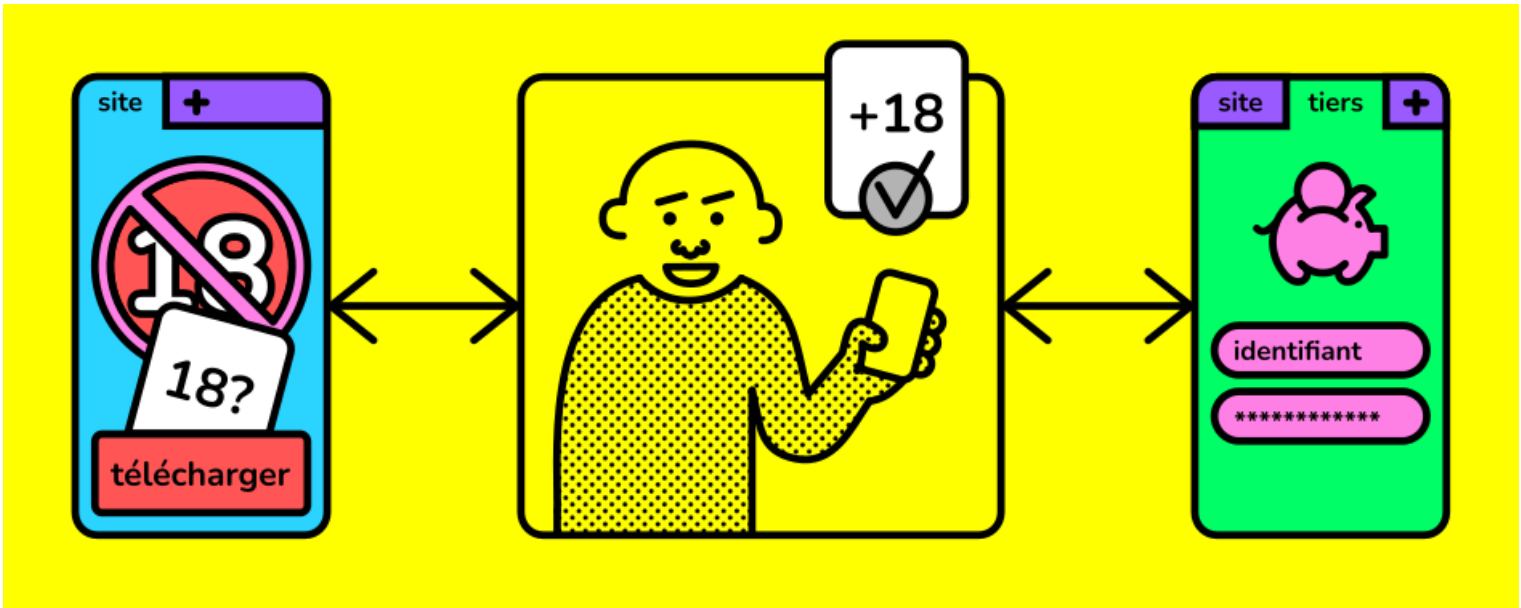
Démonstrateur du mécanisme de vérification de l'âge respectueux de la vie privée

Rédigé par Jérôme Gorin, Martin Biéri et Côme Brocas

-

21 juin 2022

Peut-on prouver qu'on est majeur sans divulguer son âge, ni son identité ? Le LINC, Olivier Blazy, professeur de l'Ecole polytechnique et chercheur en cryptographie, et le Pôle d'Expertise de la Régulation Numérique (PEReN) de l'Etat, ont développé un exemple de mise en œuvre d'un système de vérification d'âge pour permettre l'accès à certaines catégories de sites sans que ne soient partagées d'autres informations identifiantes.



Un contexte politique et d'émergence de nouveaux acteurs

L'actualité récente a relancé la question de la vérification de l'âge en ligne, qu'ils s'agissent **d'un renouveau du contrôle parental** ou de la **mise en demeure de sites à caractère pornographique**. La CNIL a déjà eu l'occasion de se pencher sur ces questions, dans sa série **de recommandations concernant les mineurs et le numérique** et en particulier sur la vérification de l'âge pour l'accès aux sites pornographiques, **dans son avis du 3 juin 2021**.

Il y avait été recommandé le recours à un système respectueux de la vie privée, mis en place par un tiers vérificateur lors du processus de vérification d'âge par les sites. L'intérêt d'une telle solution réside notamment dans la mise en œuvre de mécanismes permettant d'empêcher, d'une part, que le tiers de confiance identifie le site ou l'application à l'origine d'une demande de vérification et, d'autre part, de limiter la capacité du site à l'origine de cette demande d'identifier l'individu concerné.

Dans l'aspect pratique de la mise en œuvre d'un tel système, il y a deux dimensions à prendre en compte : d'abord la création de l'information d'âge (ou de majorité par exemple, si la vérification d'âge ne vise que des seuils : « a plus de 18 ans »), et la question de la vérification de l'âge par un service. Ces deux aspects soulèvent inévitablement des questions relatives à la sécurité, la fiabilité et à la protection des données et de la

vie privée des individus (notamment quand il s'agit d'informations relatives à une supposée orientation sexuelle). L'obtention de l'information d'âge (ou preuve d'âge) par le tiers de confiance n'est pas explicitement traitée ici et pourra faire l'objet d'une communication ultérieure. Le Pôle d'Expertise de la Régulation Numérique (PEReN) a par ailleurs consacré le n°4 de sa collection Éclairage sur…à ce sujet (**« Détection des mineurs en ligne : peut-on concilier efficacité, commodité et anonymat ? »**).

Mise en œuvre d'un démonstrateur

Dans ce sens, le LINC met à disposition la démonstration d'une solution « idéale » dans un contexte de développement des outils et acteurs de la vérification d'âge. Elle repose sur des briques de base utilisées en cryptologie sous l'expression « preuve à divulgation nulle de connaissance » ou « *zero-knowledge proof* » (voir l'encadré n°1 ci-dessous). Ces briques permettent ainsi à des personnes identifiées de prouver qu'une situation est réelle sans avoir à révéler les informations relatives à cette situation. Ce démonstrateur prouve ainsi qu'il est possible, à travers un système de tiers, de garantir la protection de l'identité de l'individu et le principe de minimisation des données.

Bien évidemment, il ne s'agit que d'une preuve de faisabilité : le fonctionnement d'une telle solution repose sur la mise en place d'un écosystème et d'une gouvernance propre et à grande échelle.

Les concepts cryptographiques mobilisés (Olivier Blazy)

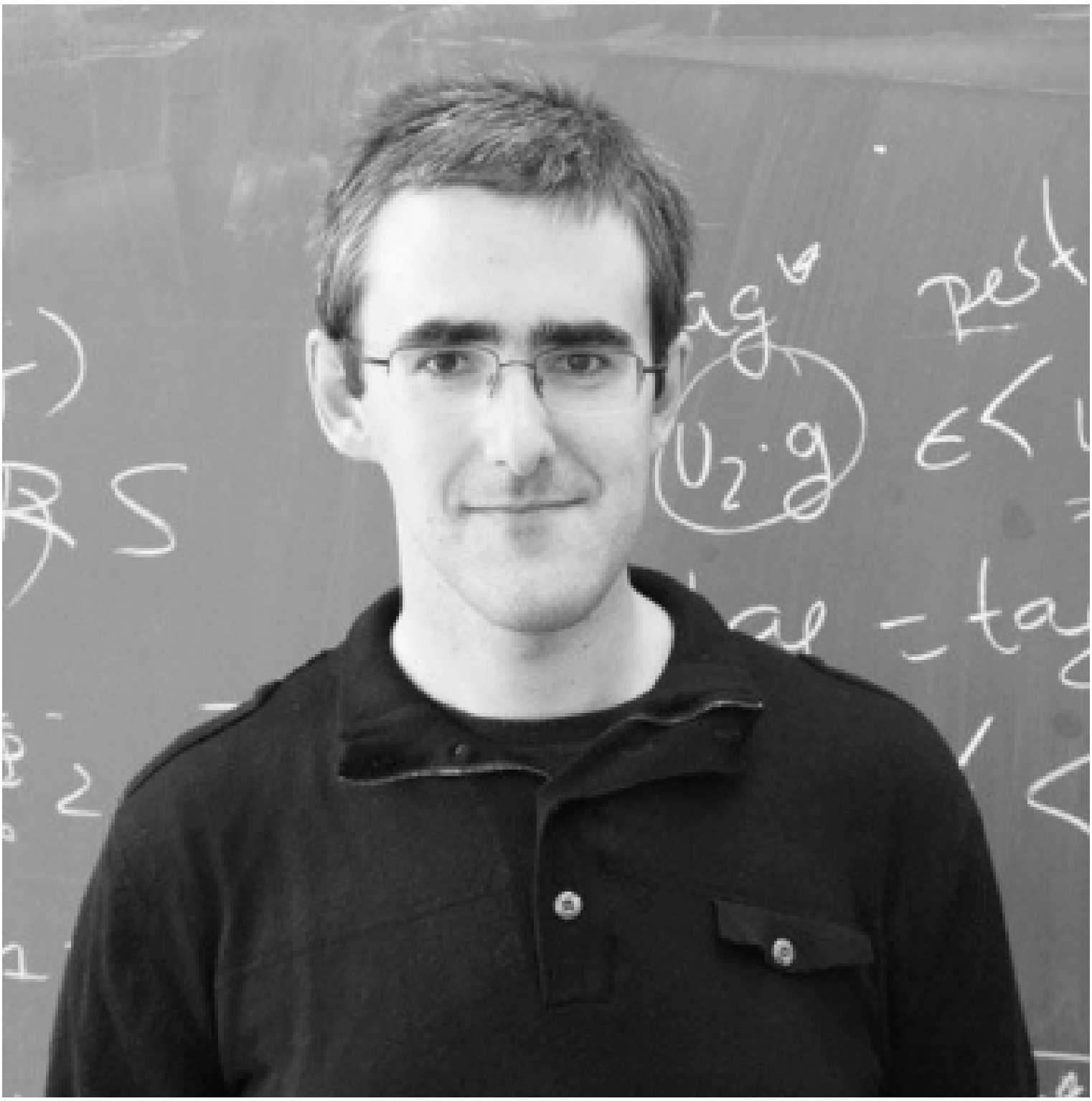
Le protocole repose principalement sur un concept cryptographique appelé « signature de groupe ». En termes cryptographiques, cette primitive permet à un utilisateur de signer anonymement au sein d'un groupe. Le terme « anonymement » est à prendre au sens cryptographique ici, au sens RGPD on parlerait de pseudonymat.

Etant donné une signature générée par un membre du groupe, il est impossible (hormis pour une autorité) de savoir quel membre l'a généré. Pour construire une telle primitive, nous combinons deux blocs fondamentaux en cryptographie :

- d'un côté des signatures numériques (qui permettent à quelqu'un de certifier une donnée et à quiconque de vérifier ensuite ce certificat) ;

- et de l'autre des preuves à divulgation nulle de connaissance (dites *Zero-Knowledge* ou ZK), qui permettent de prouver la connaissance d'un secret sans pour autant révéler ce dernier.

Grâce à la combinaison de ces primitives, une autorité peut générer une clé publique, ajouter des membres au groupe, en leur fournissant un certificat, valide sous la clé principale du groupe, de leur propre clé publique. Ensuite, les membres du groupe vont pouvoir signer des challenges à l'utilisateur, et ce dernier va pouvoir prouver qu'il possède une signature d'un challenge, par quelqu'un appartenant au groupe. De cette façon, les preuves ZK garantissent à la fois le pseudonymat de l'autorité qui a signé (via la propriété de ZK) et le fait que celle-ci est bien membre du groupe (via la propriété dite de *soundness*, c'est-à-dire que personne ne peut faire une fausse preuve). Ainsi, le site fournisseur de service est sûr de la validité de l'âge de l'utilisateur sans pour autant savoir qui l'a certifié.



Olivier Blazy

Olivier Blazy est professeur en cybersécurité à l'École Polytechnique dans le département informatique. Il est chercheur en cryptographie depuis 10 ans sur diverses thématiques dont la cryptographie pour la protection de la vie privée, et la cryptographie post-quantique. Au niveau national, il co-anime le **groupe de travail Codage et Cryptographie** du CNRS au sein des GDR Sécurité Informatique et Informatique-Mathématiques.

Les schémas ci-dessous permettent de comprendre comment la preuve de faisabilité fonctionne :

Pour la personne, cette fonctionnalité puisse être « à sa main » (Figure 1) ;

Plus généralement, sur l'écosystème : les différents acteurs en présence et le système de gouvernance nécessaire à son fonctionnement (Figure 2).

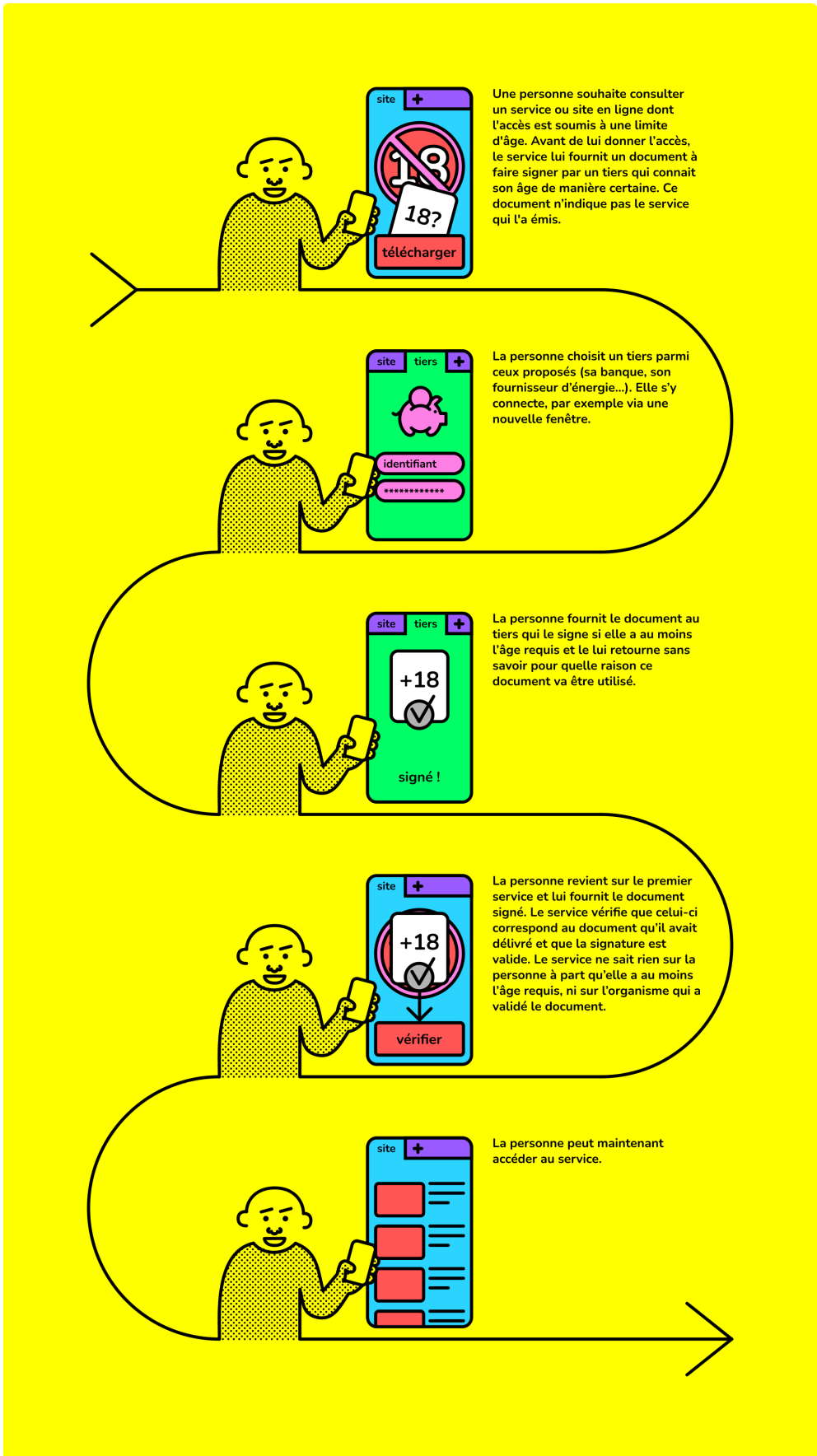


Figure 1 : Schéma du fonctionnement de la solution, du point de vue de l'utilisateur ou de l'utilisatrice.

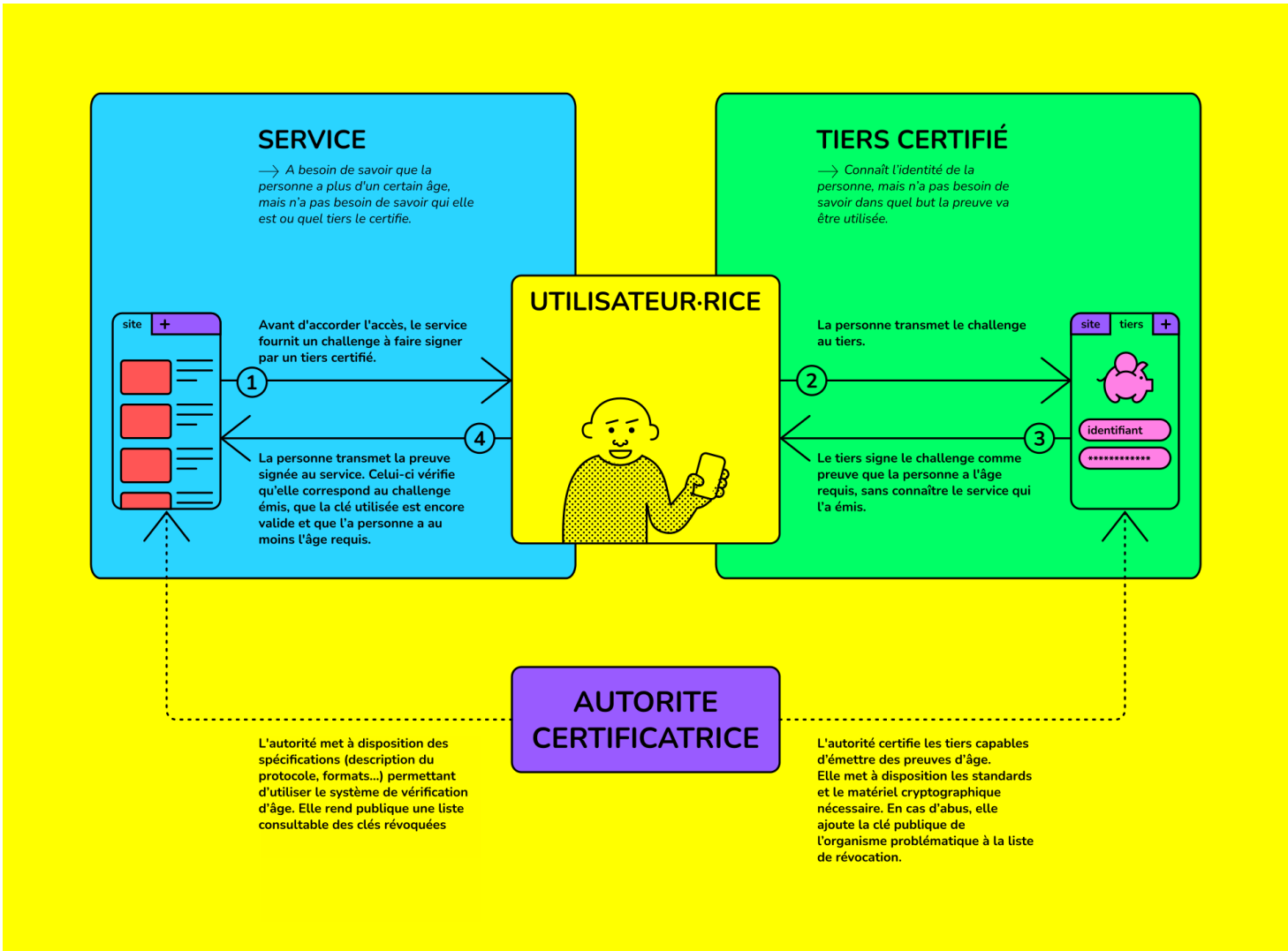


Figure 2 : Schéma du fonctionnement technique de la solution

Focus sur le démonstrateur

Pour illustrer les mécanismes mobilisés dans l'encadré précédent, le LINC met à disposition un démonstrateur sous License Ouverte sur les plateformes **Github**, **Adullact** et dockerhub.io. La conception de ce démonstrateur s'est faite en collaboration avec **Olivier Blazy** de **LIX** (c.f. supra) et pour son développement, nous nous sommes appuyés sur le **PEReN** dans le cadre d'une convention. Nous vous recommandons cette dernière solution, car elle nécessite uniquement l'installation du logiciel **Docker** et l'utilisation de la ligne de commande suivante une fois authentifié sur la plateforme :

```
docker run -p 9091:9091 -p 9092:9092 -p 9093:9093 cnil/siggroup
```

Son code est librement modifiable et réutilisable, commercialement ou non, sous réserve de mentionner la source.

Ce démonstrateur simule le fonctionnement des trois entités nécessaires à la mise en œuvre d'un échange de preuve à divulgation nulle de vérification d'âge requis, à savoir :

- un site web dont l'accès à son contenu nécessite de vérifier que l'internaute dispose de l'âge minimum requis ;

- un ou plusieurs site « accrédité (s) » pour vérifier l'âge réel des internautes ;

- une autorité « de confiance » permettant l'accréditation de ces sites.

Dans la version mis à disposition par le LINC, ces trois entités sont accessibles depuis un navigateur respectivement aux adresses suivantes : site web ou service (**https://localhost:9093**), tiers certifié (**https://localhost:9091**), autorité certificatrice (**https://localhost:9092**).

Ce démonstrateur permet d'illustrer les prérequis souhaités par la CNIL sur les procédés de vérification d'âge pour les sites reposant sur des tiers de confiance : la preuve d'âge utilisée ne comprend ni l'identité réelle des utilisateurs, ni l'identité du site utilisé pour vérifier l'âge, tout en s'assurant que le processus de vérification d'âge utilisé répond à un cahier des charges défini. Les sites accrédités pour vérifier l'âge des personnes n'ont aucune information sur le but de cette vérification, les informations de navigations et les usages de l'internaute restent confidentiels.

L'interface du site web ou du service (*par défaut localhost:9093*) permet d'initier et de télécharger un challenge à faire signer par un tiers accrédité pour vérifier l'âge des utilisateurs. Chaque challenge téléchargé est unique et associé à un âge requis et à une durée de vie limitée pour son usage.

La personne utilisant le service (ici Bob ou Alice) doit charger ces challenges sur l'interface des tiers certifiés à vérifier l'âge des internautes (*par défaut localhost:9091*). A chaque utilisateur identifié sur cette plateforme est associé un nom et un âge. Le démonstrateur dispose à l'initialisation de deux utilisateurs de test : Bob qui a 16 ans et Alice qui en a 25. L'interface de ce site permet également de créer de nouveaux utilisateurs. La signature du challenge ne peut se réaliser que si l'utilisateur dispose de l'âge requis pour accéder au site (plus de 18 ans par défaut). S'il a l'âge requis, l'utilisateur (ici, Alice) peut télécharger et transmettre le challenge signé au site web qui en vérifie la validité. La signature de ce challenge est considérée comme valide par le site si et seulement si elle émane d'un tiers accrédité par l'« autorité de confiance ». Elle ne contient en outre pas d'information permettant de révéler directement l'identité réelle de l'utilisateur.

L'interface de l'autorité certificatrice (*par défaut localhost:9092*) permet de simuler l'accréditation de nouveaux tiers habilités pour vérifier l'âge des utilisateurs. Par défaut, le démonstrateur dispose de deux tiers accrédités pour vérifier l'âge requis. Dans l'éventualité où un site tiers perd son accréditation, car son processus de vérification d'âge n'est plus en ligne avec le cahier des charges défini par l'autorité de confiance, un mécanisme de révocation permet d'invalider les signatures produites par ce dernier. Ce processus d'accréditation permet ainsi de déléguer l'audit des processus de vérification d'âge à une autorité « de confiance supérieure » ou « maître ».

Pistes d'amélioration et variations possibles

Le démonstrateur se focalise sur les apports de la signature de groupe concernant la protection de la vie privée des utilisateurs. Sa mise en œuvre nécessite aussi d'identifier les attaques potentielles sur le processus d'échange et d'y appliquer les mesures de

sécurité appropriées.

En pratique, il est également souhaitable que le challenge utilisé ne contienne pas l'information sur l'âge requis afin de limiter les possibilités de déduction du but de la vérification d'âge. Cela implique que le site accrédité puisse générer une preuve pour chaque palier d'âge possible. Par exemple, nous pouvons imaginer que cela fonctionne par grand palier selon la législation : 13 ans, 15 ans, 16 ans et 18 ans. L'utilisateur peut ainsi sélectionner depuis son navigateur le challenge signé correspondant au palier du site ou du service auquel il souhaite accéder.

Du point de vue du parcours utilisateur, l'individu doit à tout moment conserver la main sur les échanges entre les organismes afin de s'assurer de la bonne étanchéité lors de l'échange de jeton. Celui-ci doit ainsi se dérouler depuis le navigateur ou l'application de l'internaute. Ce processus de vérification pourrait être fluidifié au moyen de mécanismes d'échange automatisé de jeton d'information que l'on retrouve habituellement dans les processus de délégation d'accès (par exemple, **le protocole « OAuth »**) ou par des mécanismes d'inscription sécurisé dans le navigateur.

Enfin, les mécanismes en jeu dans le processus de vérification d'âge peuvent avoir une large visée que la vérification de la majorité : pour l'inscription sur les réseaux sociaux, l'accès à des contenus sensibles ou pour certaines ventes soumis à restrictions d'âge.

---

*Article rédigé par **Jérôme Gorin, Martin Biéri et Côme Brocas***

VOIR PLUS D'ARTICLES DE L'AUTEUR