

Port-E : Expérimentation du Portefeuille Numérique pour un Employé

Philippe Foucault, Julio Cesar Torres, Ricardo Cantu, Martin St-Pierre, Tomy Chouinard

Centre Québécois d'Excellence Numérique - Quebec's Digital Center of Excellence

Ministère de la Cybersécurité et du Numérique

Objectifs

L'objectif de cette expérimentation est de démontrer l'utilisation du portefeuille numérique en tant qu'employé dans un environnement d'expérimentation, où certaines fonctionnalités ont été simulées pour réduire la complexité. Plus précisément, nous souhaitons :

- Démontrer que l'employé peut utiliser son portefeuille numérique pour s'authentifier sur un site web d'entreprise.
- Démontrer que l'employé peut utiliser son portefeuille numérique pour déverrouiller l'accès à des portes physiques.
- Évaluer l'expérience utilisateur de l'employé lors de l'utilisation du portefeuille numérique.
- Tester la faisabilité technologique de l'identité numérique au service de l'employé.
- Évaluer la valeur de s'appliquer sa propre médecine (dogfooding) avec un cas employé avant de penser l'utiliser à plus grande échelle.

Introduction

L'expérimentation Port-E porte sur l'utilisation d'un portefeuille numérique par un employé pour accéder à ses sites web de travail et déverrouiller les portes de ses bâtiments.

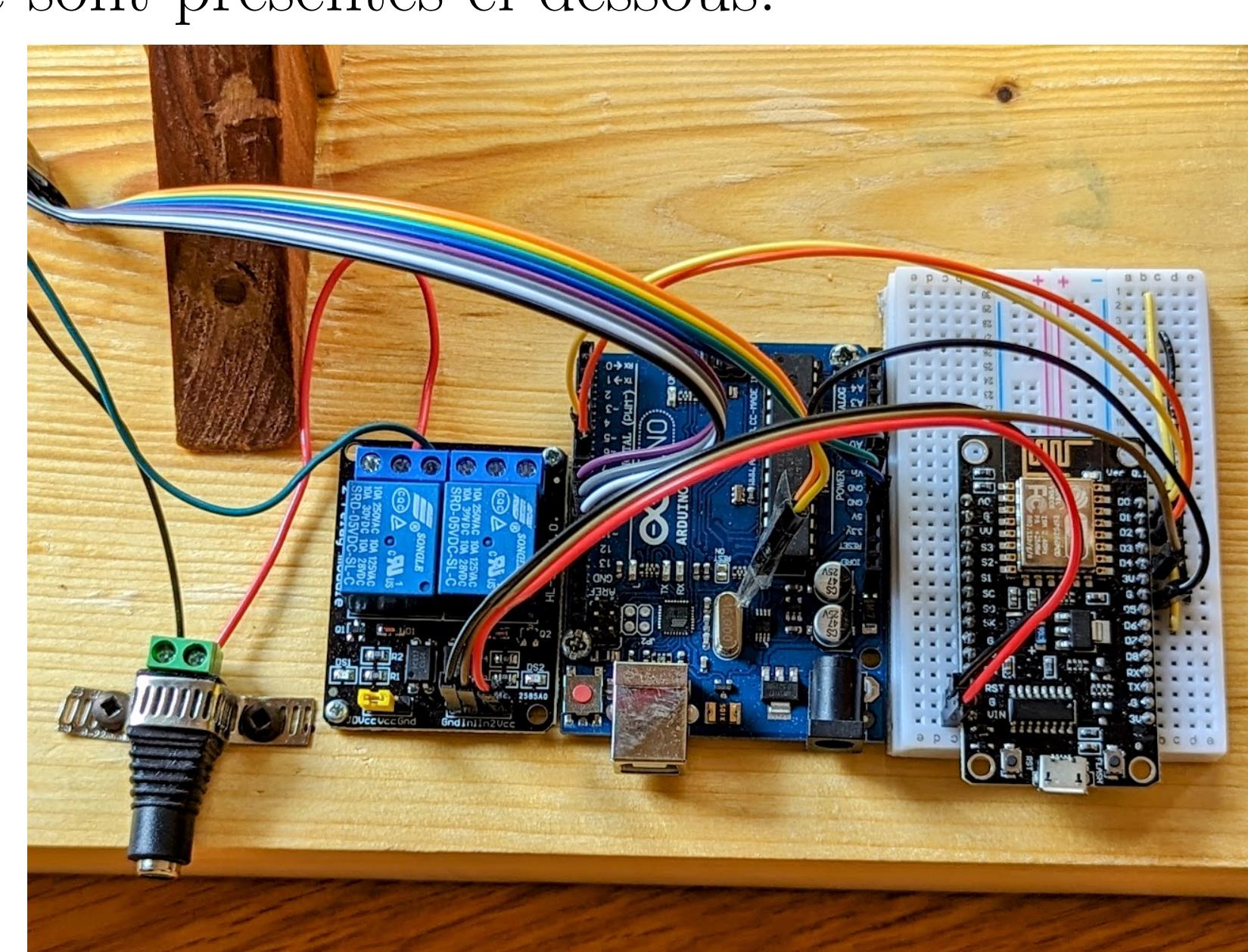
Elle repose sur l'identité auto-souveraine (SSI), une approche décentralisée qui permet aux individus de stocker leurs informations d'identité de manière sécurisée sur leur cellulaire.

L'expérimentation vise également à démontrer que si ce type de solution convient à une utilisation citoyenne, elle est également adaptée pour les employés.

Le projet, nommé Port-E, est disponible sur GitHub [1]. Port-E, inspiré du film Wall-E, signifie 'Portefeuille' dans le contexte de 'l'Employé'.

Matériaux

Les éléments utilisés pour la construction du prototype sont présentés ci-dessous:

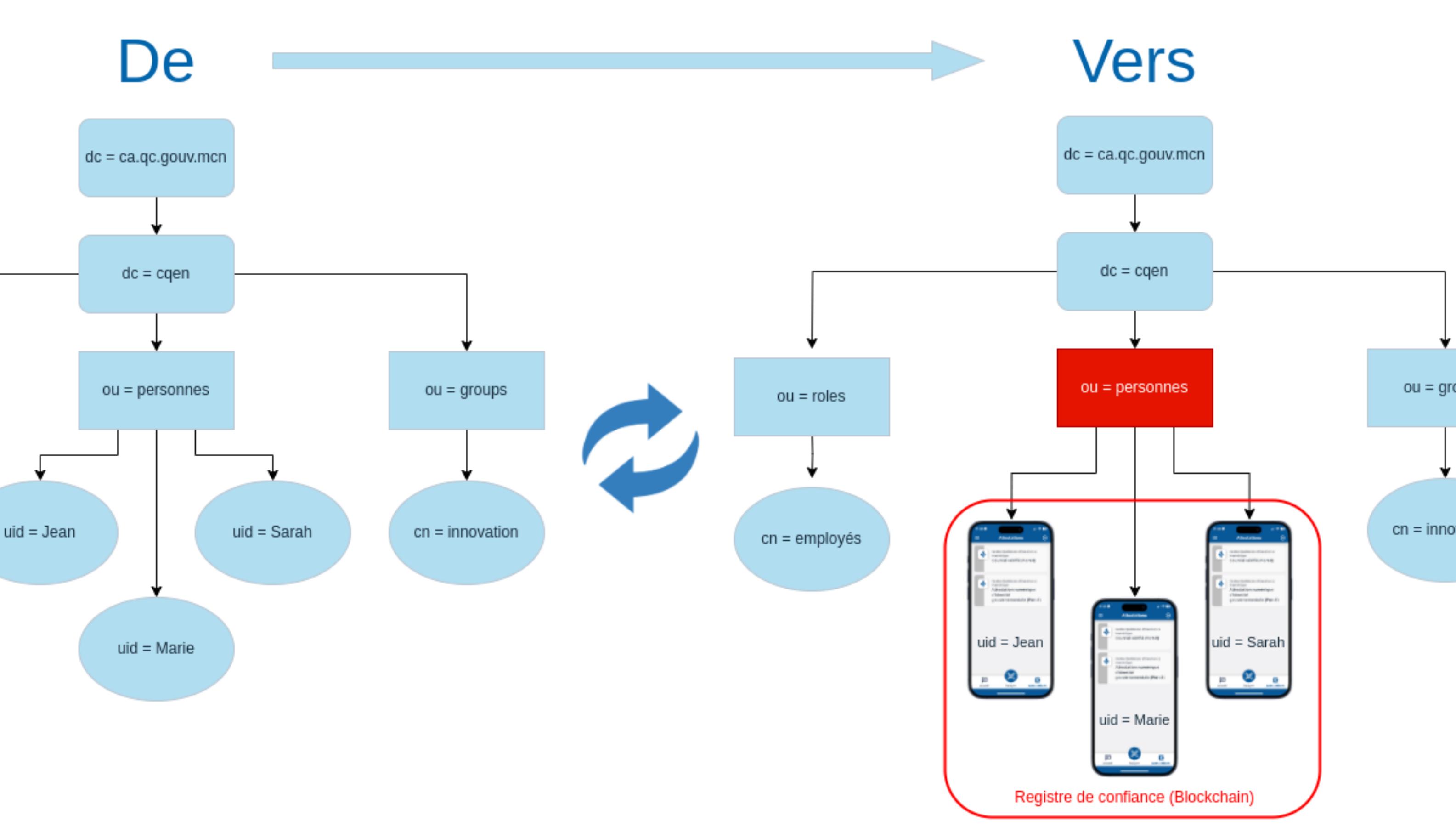
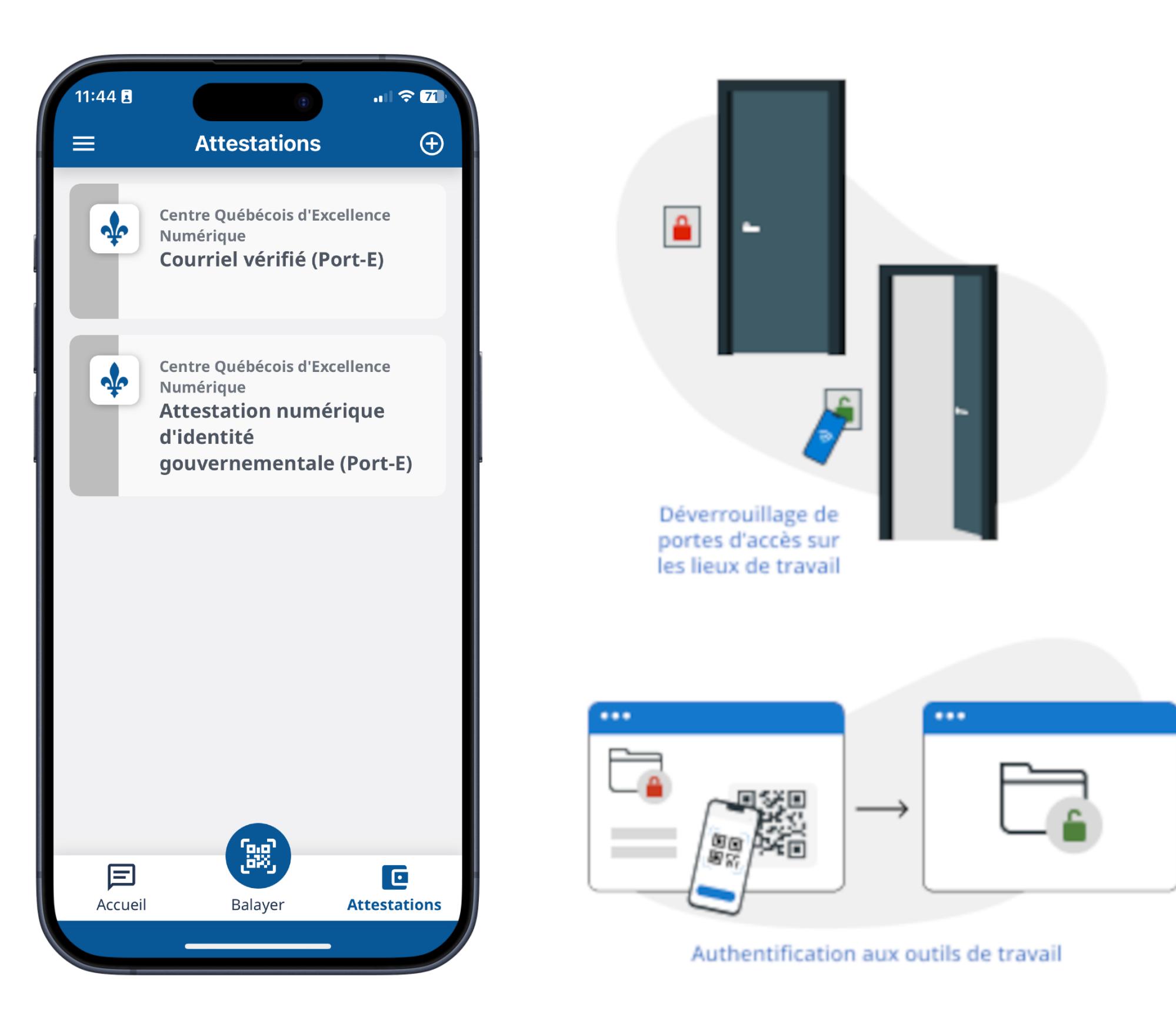


Cas d'utilisation

Le cas d'utilisation d'une attestation vérifiable pour un employé est un exemple intéressant et concret qui apporte une belle complexité. Les cas d'utilisation minimaux ont été élaborés afin de permettre la mise en place de toutes les composantes nécessaires pour expérimenter le concept sans toutefois résoudre les contraintes et particularités d'un cas d'affaires concret.

Sarah, notre employée, utilise son portefeuille numérique et obtient les attestations nécessaires qui prouvent son identité et son lien d'emploi. Par la suite, elle peut accéder au site web utilisé dans le cadre de son travail et également déverrouiller les portes d'accès sur les lieux de travail.

Nous disons au revoir aux mots de passe oubliés et à la nécessité de répondre à plusieurs questions pour s'authentifier auprès d'un prestataire de services.



Résultats

À la fin de cette expérimentation, nous avons obtenu des retours d'expérience de la part des employés sur l'utilisation du portefeuille numérique. Ces retours ont aidé à comprendre les avantages et les inconvénients de cette approche, et à identifier les améliorations potentielles.

Concrètement, deux schémas d'attestation vérifiables sont disponibles dans le portefeuille mobile de l'employé. Ils ont pour objectif de permettre :

- 1 L'émission de l'attestation d'identité.
 - d'identifier le sujet de l'attestation.
- 2 L'émission de l'attestation de courriel.
 - d'identifier la boîte de courriel sur laquelle l'employé démontre un contrôle ;
 - d'établir le lien entre la personne détentrice du courriel et son lien d'emploi lorsque la boîte de courriel est professionnelle.
- 3 La vérification permet de valider.
 - l'émission d'une requête de présentation exigeant la présentation des valeurs des attributs de l'attestation d'identité de Sarah ;
 - la présentation du courriel professionnel dont Sarah a le contrôle.

Menace pour la validité

• **Menace pour la validité interne:** sont des facteurs qui peuvent affecter des variables indépendantes ou qui n'ont pas été prises en compte lors de l'expérimentation. Certaines fonctionnalités qui ne sont pas le sujet final de l'expérimentation, telles comme les interactions avec un système de gestion d'identité et d'accès ou les interactions avec des panneaux de contrôle de porte réelles ont été simulées avec le but de réduire la complexité de l'implémentation.

Perspectives et travaux futures

- **L'intelligence artificielle (IA)** et la **blockchain** jouent un rôle crucial dans la **transformation numérique de l'administration publique**. Nous devons expérimenter ces technologies dans nos processus internes pour mieux comprendre leur potentiel et leurs défis avant de les appliquer à grande échelle dans les services publics.
- **La sécurité et la confidentialité des données** sont des préoccupations majeures dans l'application de l'IA et de la **blockchain**. Nous devons protéger les données personnelles et assurer la sécurité des systèmes contre les menaces potentielles. Les blockchains d'identité visent surtout à préserver la confidentialité des données personnelles, n'enregistrant que des **empreintes** des données réelles "*on-chain*", tout en conservant les vraies données "*off-chain*", dans les dispositifs des utilisateurs.
- L'IA peut être utilisée pour améliorer la **gestion des bâtiments intelligents**, optimiser l'utilisation de l'énergie et améliorer le confort des occupants; l'utilisation de caméras pour s'assurer qu'un employé n'a pas été suivi par une autre personne lors de son accès. Cela pourrait améliorer la sécurité tout en minimisant les inconvénients pour les employés.
- L'évaluation de la **mise à l'échelle** de l'expérimentation sera réalisée ultérieurement, en tenant compte de la complexité des **environnements technologiques** et des processus d'affaires qui seront alors évalués en collaboration avec les équipes de réalisation.

Conclusion

L'expérimentation a démontré que l'usage d'un portefeuille numérique par les employés dans un environnement contrôlé d'expérimentation est non seulement réalisable, mais aussi très pratique.

L'expérimentation a permis d'explorer les aspects techniques du contrôle d'accès aux ressources, tant virtuelles que physiques, et d'évaluer les modèles soutenant ce contrôle. Le courriel a été utilisé comme preuve du lien d'emploi, car l'employeur connaît cette relation et a déjà identifié au préalable l'employé.

L'organisation émet une attestation vérifiable prouvant ce lien. L'accès physique a présenté des défis, notamment la taille des paquets NFC, résolus en utilisant un URL shortener.

En conclusion, l'utilisation d'un portefeuille numérique pour les employés est relativement simple dans un environnement d'expérimentation, car les règles d'utilisation sont déjà bien définies. L'identité numérique facilite l'application de ces règles.

Il convient de souligner que les conclusions tirées de cette expérimentation doivent être prises en compte avec prudence lors de la mise en œuvre d'une application réelle.

Information Additionnelle

Le prototype utilise la blockchain panaqué que nous opérons le Québec, l'Ontario et la Colombie-Britannique basé sur la technologie Hyperledger Indy.

Nous avons utilisé un portefeuille numérique pré-configuré dans le prototype basé sur les technologies Hyperledger Aries Framework Javascript (AFJ) et Hyperledger Aries Mobile Agent React Native (Bi-fold).

Références

- [1] P. Foucault, R. Cantu, J. Cesar Torres, M. St-Pierre, and T. Chouinard. Expérimentation sur l'utilisation d'un portefeuille mobile en tant qu'employé, 2023. <https://github.com/CQEN-QDCE/exp-port-e> [Accessed: (2024-01-19)].

- [2] Tom Igoe, Don Coleman, and Brian Jepson. *Beginning NFC: Near Field Communication with Arduino, Android & PhoneGap*. O'Reilly, 1st edition, 2023.

- [3] Hyperledger Foundation. Hyperledger aries. <https://www.hyperledger.org/projects/aries> [Accessed: (2024-01-22)].

Remerciements

Un grand merci à toutes les personnes et projets de code source libre dont le code a été utilisé. Merci à la Colombie-Britannique pour l'inspiration.



Coordonnées

- Email: cjen@mcn.gouv.qc.ca

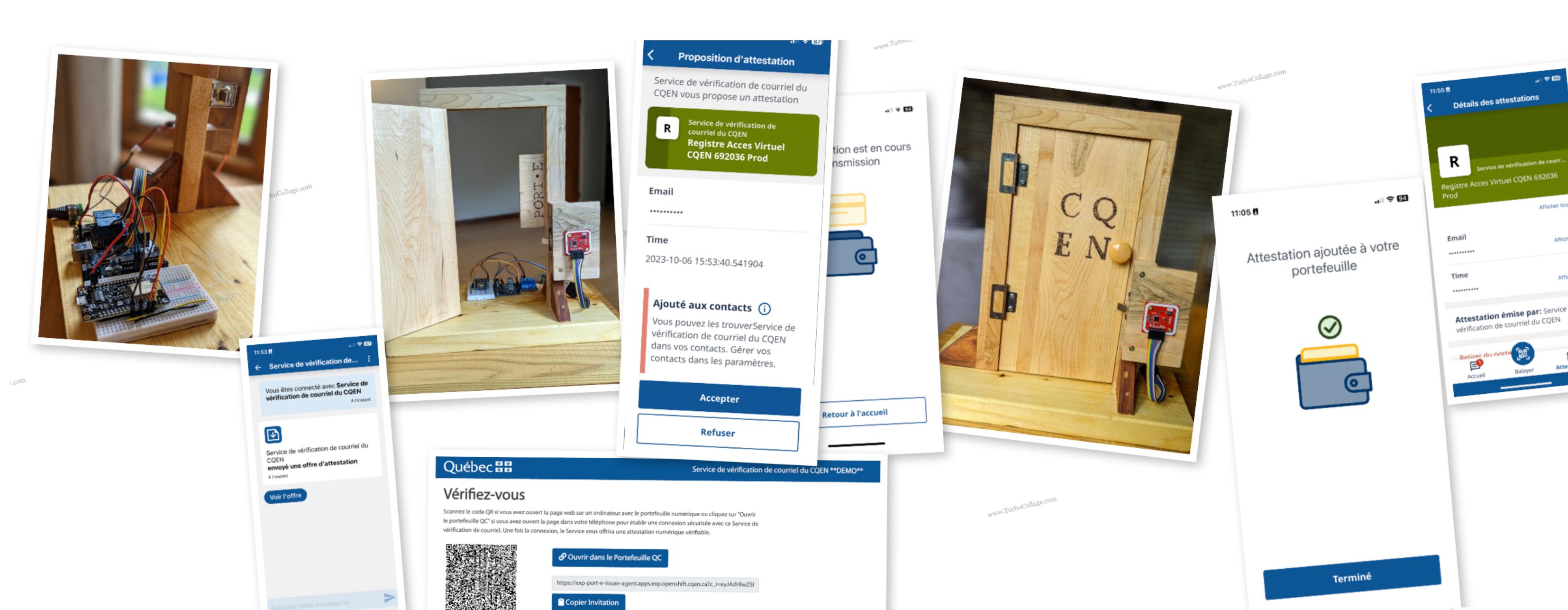


Figure 2 : L'attestation vérifiable auto-déclarée d'identité numérique

```
"txn": {
  "data": {
    "data": {
      "attr_names": [
        "credentialSubject.firstName",
        "credentialSubject.lastName"
      ],
      "name": "Attestation numérique d'identité gouvernementale (EXP)",
      "version": "0.0.7"
    }
  }
}
```

Figure 3 : L'attestation de preuve de contrôle de sa boîte de courriel