Developing User Interfaces for Verifying Digital Personhood Credentials

1. Background

With the rapid rise in AI-generated activity, it's anticipated that humans will soon become the minority presence online. Furthermore, while anonymity has long been a core value of the internet, it has also enabled bad actors to exploit fake or misleading identities for fraud, disinformation, and other deceptive practices. As AI systems increasingly mimic human behavior—solving CAPTCHAs or generating lifelike videos—traditional identity verification methods are losing their effectiveness. To safeguard human users in a future where AI may dominate digital spaces, we need innovative solutions to reliably distinguish real people online.

2. Project Description

This project seeks to develop privacy-preserving technology that allows individuals to prove their humanity without exposing personally identifiable information. The primary objective is to build a robust front-end identity ecosystem (backed by a decentralized identity infrastructure that will be developed in parallel by external but related teams) that supports seamless user journeys for issuing, storing, and presenting verifiable personhood credentials. Key components of this ecosystem include:

1. **Accessible onboarding flows** that guide users through the credential issuance process with transparency and ease,
2. **User-friendly credential wallet (app)** for secure storage and management, and
3. **Intuitive verification interfaces** that enable credential presentation of selected identity credentials to online social platforms

2.1. Project Goals

Build a Front-End Identity Ecosystem: Create a cohesive set of interfaces and workflows that support the user journeys through:

- Credential issuance
- Secure storage of verifiable credentials locally in the user's device through digital wallet apps (smilar to Apple or Google Wallet)
- Verifiable presentation that enables transfer of selected identity credentials to online social platforms
- Ensure the system is accessible and intuitive for non-technical users.

2.2. Other requirements

- Design with future internet infrastructure in mind, ensuring compatibility with decentralized identity (DID) standards (e.g., W3C VC/DID).
- Support integration with various platforms, browsers, and digital services.
- End-to-end encryption for all credential exchanges.

- Minimal data exposure—no raw biometric or personal data should leave the user's device.
- Smooth onboarding process that balances ease of use with strong verification.
- Responsive UI/UX optimized for both mobile and desktop platforms.

2.3. Ethical Requirement

All team members will be required to sign a non-disclosure agreement (NDA) upon onboarding to ensure confidentiality and responsible handling of project-related information.

3. **Desired Skill Set**

- Taking/taken courses: CSCI 474, 475
- Programming languages such as: Python, JavaScript, PHP, HTML
- Frontend frameworks such as: React, Angular
- Android and/or iOS app development
- UI/UX Design tools like Figma, Sketch, or Adobe XD.

4. **Preferred Team Size**: 4 students

5. **Location of Work**: Mines Campus

6. **Primary Client Liaison**: Dr. Alemitu Bezabih, Research Associate (Additional Collaborators: Prof. Estelle Smith, Prof.Guannan Liu, Prof. Chuan Yue, Anhao Xiang)