1. Introduction

This document outlines the product requirements for a new system component designed to create and validate 1 to 5 social media accounts for a solopreneur. The primary objective is to enable the creation of unique, non-linked accounts on platforms like TikTok and Instagram, mitigating the significant risk of account bans. The system is designed with a "human-in-the-loop" model, ensuring that a human operator retains final authority over critical actions.
It is crucial to state that the creation and management of multiple social media accounts to circumvent platform policies is a high-risk activity that directly violates the Terms of Service of platforms like TikTok and Instagram. The system specified below is built with a calculated risk in mind, leveraging best practices from the underground communities of social media developers to maximize the probability of success while acknowledging the certainty of a technological arms race with the platforms' anti-bot detection systems.

2. Goals & Objectives

- **Primary Goal:** Enable the solopreneur to create and manage 1 to 5 social media accounts (initially TikTok and Instagram) as unique, independent profiles to avoid account linking and subsequent suspension.
- **Objective 1:** Implement a guided, step-by-step account creation wizard that simplifies the technical complexity for a non-expert user.
- **Objective 2:** Integrate a digital fingerprinting solution to ensure each account is created from a distinct digital identity, preventing platforms from linking them to a single user or IP address.
- **Objective 3:** Establish a clear "warm-up" protocol that requires human intervention to mimic authentic user behavior, reducing the likelihood of immediate detection and a ban.

3. Functional Requirements

FR-1: Account Creation Wizard

- The system shall provide a user-friendly wizard interface for creating new accounts.
- The wizard must prompt the user for essential account details, including a unique email address for each new account to prevent linking.
- The wizard will allow the user to select the target platform (TikTok or Instagram).

FR-2: Automated Digital Identity Management

- The system shall automatically assign a unique residential or mobile proxy to each new account to provide a distinct IP address, making the traffic appear to originate from a real user.
- The system shall integrate with an anti-detect browser (e.g., BitBrowser) to create and manage a unique digital fingerprint for each account, including distinct browser versions, operating systems, and geolocation data.

FR-3: Guided "Warm-Up" Protocol

- After an account is created, the system must present a clear, actionable checklist for a manual "warm-up" period of at least 48 hours.
- The checklist shall include specific daily tasks, such as:
    - Spending approximately 15 minutes a day scrolling through the feed and liking a few posts.
    - Following a small number of accounts.
    - Leaving comments with emojis to simulate human-like interaction.
- The system shall recommend using mobile cellular data for the initial setup and warm-up to enhance the appearance of authenticity.
- On day 3, the system will prompt the user to create a video or post using the platform's native tools to improve visibility and avoid a "bot-like" profile.

FR-4: Human-in-the-Loop Validation

- The system shall not automate any actions on a new account until the user has manually confirmed that the account has passed its "warm-up" period.
- A dashboard will display the status of each account (e.g., "New Account Created," "In Warm-up Period," "Ready for Validation," "Validated").
- The user must manually validate the account by clicking a

button after reviewing its activity and ensuring it appears authentic and human-like.

4. Technical Specification

4.1. Architecture

A new microservice, the **AccountCreationService**, will be developed and integrated into the existing system. This service will be responsible for all account-related tasks, operating independently of the main Action Engine. This modular architecture ensures that a failure or ban related to account creation does not impact the core automation logic of the rest of the system.

4.2. Components

Component	Functionality	Suggested Technology
AccountCreationService	Manages the account creation workflow. It orchestrates the creation of unique digital fingerprints and the execution of account-related tasks via unofficial APIs or web scraping frameworks.	Python, Flask/ FastAPI
ProxyManager	A dedicated service that provisions and manages a pool of residential proxies, assigning a unique IP address to each new account to avoid IP blacklisting and linking.	Python, Proxy API clients

FingerprintManager	Interacts with an anti-detect browser's API to generate a unique digital profile for each account. This includes managing browser type, version, operating system, and screen resolution.	Python, BitBrowser/ anti-detect API
PlatformServices	The existing microservices (e.g., TikTok Service, Instagram Service) will be extended to include the initial account creation and login logic. This will use unofficial, reverse-engineered methods like cURL or headless browsers.	Python, Playwright, cURL
Data Persistence	A relational or NoSQL database to store account credentials, proxy assignments, and a boolean flag indicating whether the account has been manually validated.	PostgreSQL or MongoDB

4.3. Workflow

The user will initiate the process through the UI. The request is sent to the AccountCreationService, which:

1. Requests a unique proxy from the ProxyManager and a unique digital fingerprint from the FingerprintManager.
2. Uses the PlatformService (e.g., the Instagram Service) to

create the new account using the assigned proxy and digital fingerprint.
3. Upon successful creation, it stores the account credentials and sets a status of "In Warm-up."
4. The UI displays the warm-up checklist and a button for manual validation.
5. After the user completes the warm-up and clicks "Validate," the AccountCreationService updates the account status to "Validated," making it available for the core automation functions.

5. Risks and Disclaimers

- **Policy Violation:** This system's core functionality is a direct violation of platform Terms of Service. The most likely outcome of a detected violation is a permanent account ban, which would result in the irrecoverable loss of the solopreneur's digital brand presence and audience.

- **Fragility and Maintenance:** The reliance on unofficial, reverse-engineered APIs and web scraping makes this system extremely fragile. A minor platform update could render the entire system inoperable, requiring significant and unquantifiable manual labor to fix.

- **Detection by AI:** Social media platforms use sophisticated AI and machine learning to detect coordinated and non-human behavior. While digital fingerprinting and proxies help, there is no guarantee against detection. The system is designed to delay, not prevent, the inevitable arms race with platform security.

6. Success Metrics

- **Metric 1:** Number of accounts successfully created and validated through the system.
- **Metric 2:** The percentage of created accounts that remain active (not banned or shadowbanned) for a 30, 60, and 90-day period.
- **Metric 3:** User feedback on the clarity and effectiveness of

the guided "warm-up" process.