# **Summary of Feature: Biometric Liveness Detection for SSI Authentication**

***The Issue: Preventing Bot-Based Attacks in SSI Authentication***

In conventional systems, bots can mass-register and create fake accounts using automation tools. These systems often rely on solutions like CAPTCHA or bot detection software to mitigate such attacks. However, **Self-Sovereign Identity (SSI) systems** face a similar risk because:

1. **DIDs can be mass-generated** by malicious actors.
2. Bots can create legitimate Verifiable Credentials (VCs) and pass standard ownership, integrity, and authenticity checks during login.
3. Current SSI-based systems typically lack integrated **bot detection** mechanisms.

To address this gap, we propose **Biometric Liveness Detection (BLD)** as an additional step to ensure that only real users (not bots) can access accounts.

**How It Works:**

1. **QR Code Challenge**:
2. The user scans a QR code to initiate the SSI-based login process.
3. The verifier sends a **nonce** (a one-time challenge value) to ensure session freshness.
4. **Biometric Liveness Verification**:
5. The user’s device prompts for a **real-time biometric scan** (e.g., fingerprint or facial recognition).
6. The biometric scan is processed securely within the device's **Secure Enclave** or **Trusted Execution Environment (TEE)**.
7. The system:
8. Combines the **nonce** (challenge) with the scan result.
9. Generates a **hash** and **signs it** using the device's private key.
10. **Proof Validation**:
11. The verifier receives the signed hash and performs the following checks:
12. Verifies the signature to confirm the proof originated from a trusted device.
13. Ensures the nonce is fresh and valid (proving the scan occurred in real time).
14. Validates the hash integrity to confirm the biometric data is fresh and untampered.

**Key Benefits:**

* **Prevents Bot Attacks**: Ensures that only real users with live biometric verification can complete the login process.
* **Real-Time Liveness Detection**: Nonce-based hashing guarantees that biometric scans are performed **during the current session**.
* **Privacy-Preserving**: Raw biometric data **never leaves the device** and is securely handled within the Secure Enclave/TEE.
* **Combines SSI with Biometrics**: Adds a strong **liveness verification layer** while preserving the decentralized and user-controlled nature of SSI.

# **Summary of Feature: Account Center for Seamless SSI Login**

***The Issue: Streamlining the SSI Login Process for Better User Experience***

While SSI-based login systems provide enhanced security and user control, the process can feel cumbersome for users:

1. Scanning a QR code every time for login may become tedious.
2. Manually selecting the correct Verifiable Credential (VC) adds unnecessary complexity, especially for users with multiple accounts.
3. Switching between apps for authentication disrupts the user experience.

To address these issues, we propose an **Account Center** feature, a centralized hub within the SSI wallet that streamlines and automates the login process.

**How It Works:**

1. **Centralized Application Display:**
   * The Account Center page in the wallet showcases all installed applications on the user’s device that support SSI login (e.g., TikTok, Maybank, Netflix).
   * Each application is displayed as an interactive widget for quick access.
2. **Application Grouping for Organization:**
   * Users can group applications into customizable categories, such as "Banking" (e.g., Maybank, CIMB), "Social Media" (e.g., TikTok, Instagram), and a default "Others" for non-sorted applications.
   * These groups improve organization and allow users to locate and access their desired applications faster.
3. **Single-Click Login:**
   * Users simply click on the desired application widget to initiate login.
   * The wallet automatically presents the appropriate Verifiable Credential (VC) to the verifier without requiring manual selection by the user.
4. **Multi-Account Management:**
   * If a user has multiple accounts for the same application, they are prompted to select the desired account before logging in.
   * The wallet ensures the correct VC is used based on the selected account.
5. **Automatic Redirection:**
   * After successful verification, the user is seamlessly redirected to the home page of their account within the selected application, bypassing the need for manual intervention.

**Key Benefits:**

* **Convenience:** Eliminates the need for QR code scanning and manual VC selection, enabling faster and more efficient logins.
* **Efficiency:** Consolidates all SSI-enabled applications into a single, user-friendly interface.
* **Personalization:** Allows users to manage multiple accounts for the same application effortlessly.
* **Enhanced Organization:** Application grouping provides a clean, structured way to access apps, reducing clutter and improving navigation.
* **Enhanced User Experience:** Streamlines the authentication process, reducing friction and making SSI adoption more appealing.

**Summary Impact:**  
The Account Center transforms the SSI wallet into a dynamic, user-centric hub for secure, organized, and seamless authentication across applications, delivering unparalleled convenience and usability.

# **Summary of Feature: Credential Leasing for Temporary Access with Smart Contracts**

***The Issue: Limited Flexibility in SSI Credential Sharing***

In traditional SSI systems, Verifiable Credentials (VCs) are tightly bound to their owners. While this ensures security and user control, it limits flexibility:

1. Owners cannot temporarily share their credentials with trusted parties for account access.
2. Shared VCs fail ownership verification, preventing their use by others.
3. No standard mechanism exists for secure, time-bound credential sharing in SSI systems.

To address this limitation, we propose the **Credential Leasing feature**, enabling users to securely and temporarily share access to their credentials using **blockchain-based smart contracts**.

**How It Works:**

1. **Credential Leasing Process:**
   * The owner selects a Verifiable Credential (VC) to lease.
   * Specifies the lessee (identified by their DID) and chooses a lease duration (manual revocation or time-based).
   * A lease record is created and stored on the blockchain using **smart contracts**, ensuring transparency and tamper-proof validation.
2. **Lease Metadata:**
   * **Lease ID:** Unique identifier for each lease.
   * **Owner DID:** The original credential owner's decentralized identifier.
   * **Lessee DID:** The lessee's decentralized identifier.
   * **Credential Identifier:** The identifier of the VC being leased.
   * **Lease Period:** Either time-based with an expiration timestamp or manually revocable.
   * **Revocation Status:** Indicates whether the lease has been revoked.
3. **Verification and Access:**
   * Lessee provides the lease details when attempting to access an account.
   * The system checks the lease validity through the **smart contract** by verifying:
     + Ownership of the lease by the lessor.
     + Lessee’s DID matches the lease record.
     + Lease expiration status.
     + Revocation status.
   * Upon successful validation, the lessee gains access to the account linked to the leased VC.
4. **Lease Management:**
   * Owners can revoke active leases at any time through the **smart contract**, ensuring ongoing control.
   * Time-based leases automatically expire upon reaching their defined duration.

**Key Benefits:**

* **Flexibility:** Enables temporary access to accounts without compromising ownership or security.
* **Transparency:** **Smart contract-based records** ensure leases are tamper-proof and verifiable.
* **User Control:** Owners retain full authority over lease creation, management, and revocation.
* **Efficient Collaboration:** Facilitates shared access for use cases like corporate account delegation or temporary service access.
* **Alignment with SSI Principles:** Preserves decentralization and user sovereignty while enhancing functionality.

**Summary Impact:**

The Credential Leasing feature enhances the adaptability of SSI systems by using **smart contracts** to enable secure, temporary, and controlled sharing of credentials. It broadens the scope of SSI applications, offering users and organizations greater flexibility while maintaining the integrity and trust of decentralized identity systems