REPUBLIC OF SOUTH AFRICA | REGISTER OF PATENTS | PATENTS ACT, 1978

Official application No.	Lodging date: Provisional	Acceptance date
21 01 2026/03023	22 2026/03/18	47
International classification	Lodging date: Complete	Granted date
51	23	

71 Full name(s) of applicant(s)/Patentee(s):

Paul Armer
Parkada Farm, D176, Ballito, 4399, South Africa

71 Applicant substituted:	Date registrered
71 Assignee(s):	Date registrered

72 Full name(s) of inventor(s):

Paul James Armer

Priority claimed:	Country	Number	Date

54 Title of invention

HARDWARE-BACKED BIOMETRIC SESSION INJECTION FOR MODERN AND LEGACY ENVIRONMENT PASSWORD OBSOLETION.

Address of applicant(s)/patentee(s):

Parkada Farm, D176, Ballito, 4399
SOUTH AFRICA

74 Address for service

DEBRA RAY ARMER
Parkada Farm, D176, Ballito, 4399
SOUTH AFRICA
Reference No.

61 Patent of addition to No.	Date of any change
Fresh application based on.	Date of any change

Form P6

REPUBLIC OF SOUTH AFRICA

PATENTS ACT, 1978

PROVISIONAL SPECIFICATION

(Section 30(l) - Regulation 27)

Official Application No.		
21	01	

Lodging Date
22

Full name(s) of applicant(s)
71

Full name(s) of inventors(s)
72

Title of invention
54

(RP42E)

PROVISIONAL SPECIFICATION

1. TITLE OF THE INVENTION

Hardware-Backed Biometric Session Injection for Modern and Legacy Environment Password Obsoletion.

2. FIELD OF THE INVENTION

This invention relates to an authentication system and method for obsoleting passwords and password managers by leveraging hardware-backed biometric verification to inject authenticated sessions into modern and legacy computing environments.

3. BACKGROUND TO THE INVENTION

Traditional digital security relies on centralized databases of "secrets" (passwords) or local "vaults" (password managers). Both architectures are vulnerable to data breaches, phishing, and human error. Furthermore, many users suffer from physiological biometric failure, where fingerprints or facial recognition are unreadable, rendering standard biometric systems unreliable. There exists a need for a system that provides total identity autonomy while remaining compatible with legacy (e.g., PHP 5.6) environments and providing a recovery path that does not compromise security.

4. SUMMARY OF THE INVENTION

The present invention provides a system and method for obsoleting passwords by eliminating the requirement for a stored "Secret." Traditional authentication relies on a "Vault" containing encrypted credentials decrypted via a Master Password. The present invention replaces this with a **Just-In-Time (JIT) Identity Generation** model.

By leveraging Hardware-Backed User Verification (10), the user’s physical device acts as a **Dynamic Key Generator**. Upon request from the Bridge Interface (14), the device produces a high-entropy cryptographic signature—verified by Biometric or Secure PIN (12)—transformed into a single-use Cryptographic Proof (18).

The invention further provides a **Cross-Domain Auto-Provisioning** method, wherein a successful verification of the Cryptographic Proof (18) triggers the automated creation of a user account within the Vendor Environment (22) without manual data entry. Additionally, the system includes a **Hardware-Agnostic Recovery Protocol**, allowing a user to overwrite an obsolete hardware-bound credential with a new device enrollment via an atomic reset of the identity record in the Centralized Vault (16), maintaining 100% availability during device migration or loss.

5. BRIEF DESCRIPTION OF DRAWINGS

FIG. 1 is a flowchart illustrating the hardware-backed biometric session injection process, the hardened server-to-server handshake, and the automated user-provisioning loop.

6. DETAILED DESCRIPTION OF THE INVENTION

The present invention utilizes a Hardware-Backed User Verification (UV) protocol to establish identity without a centralized password database. The system prioritizes Class 3 (Strong) biometric authenticators stored within the device's Secure Enclave.

In cases of **Physiological Biometric Failure**, the invention employs a Hardened Fallback Logic. When the system requests a userVerification: required state, the User Device (10) evaluates the strongest available local authenticator, such as a hardware-protected Device PIN. Because the PIN is verified within the Trusted Execution Environment (TEE) and tied to physical anti-brute-force mechanisms, it satisfies the requirement for a Cryptographic Signature.

The system further utilizes a **Hardened API Handshake (20)**. A server-to-server validation occurs where the Vendor Environment (22) sends the Cryptographic Proof (18) and a unique Vendor API Key to the Centralized Vault (16). Upon successful validation, the vendor environment performs **Just-In-Time Provisioning**: if the verified identity does not exist in the local database, a new user record is automatically generated, injecting an Authenticated Session (24) into the user’s browser.

To resolve device loss, the Centralized Vault (16) implements a **Credential Replacement Logic**. When a 'NotFoundError' is detected by the Bridge Interface (14), a 'force_reset' command is triggered. This executes an atomic deletion of the existing hardware-bound credential, permitting a fresh enrollment and re-linking the user's identity to new hardware without compromising Zero-Knowledge integrity.

7. EXAMPLES OF USE

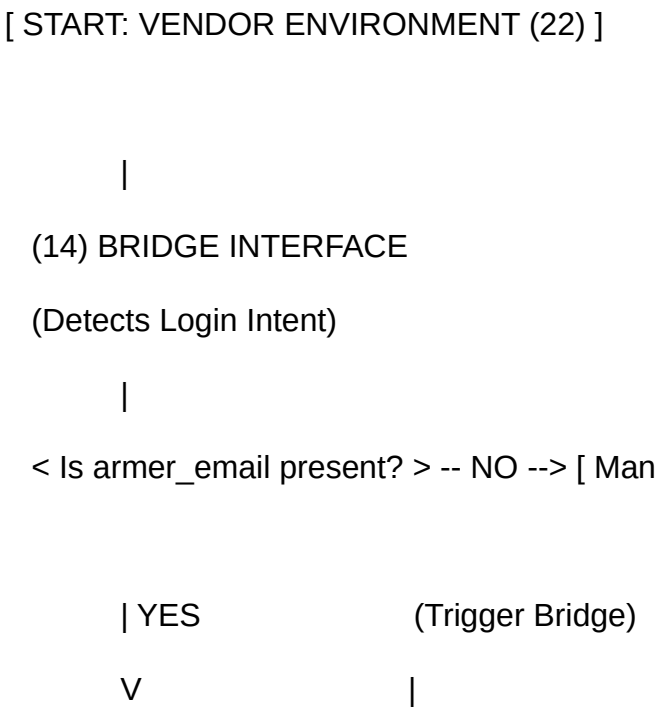
A user with unreadable fingerprints accesses a legacy vendor site on a Samsung A26. The Bridge Interface (14) triggers a Hardware-Backed UV (10). The device prompts for a Secure PIN (12), releasing a signature to the Centralized Vault (16). A Cryptographic Proof (18) is validated via a Hardened API Handshake (20). If the user is new, the Vendor Environment (22) auto-registers the account and creates an Authenticated Session (24). If the user has a new device, the system triggers a Credential Replacement flow to update the vault.

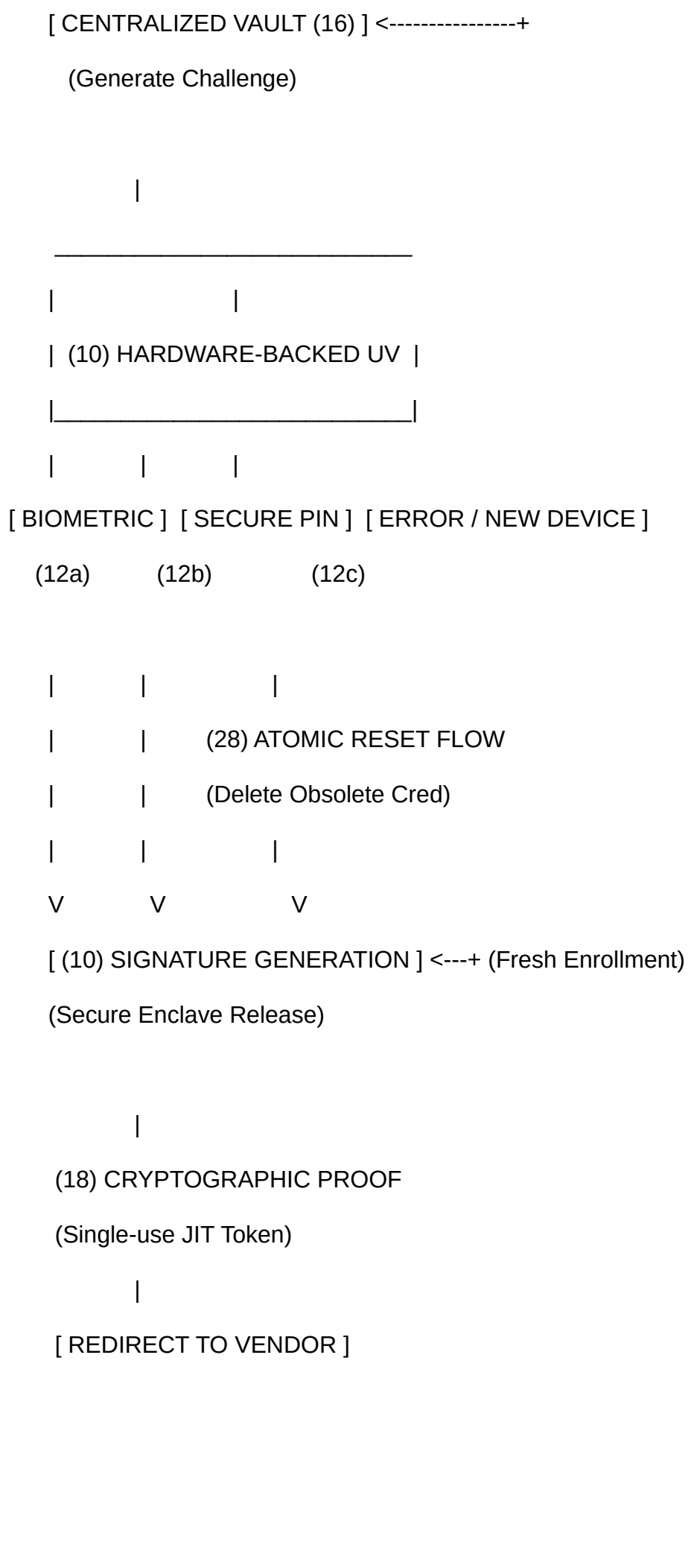
8. DRAWING 1: SYSTEM ARCHITECTURE

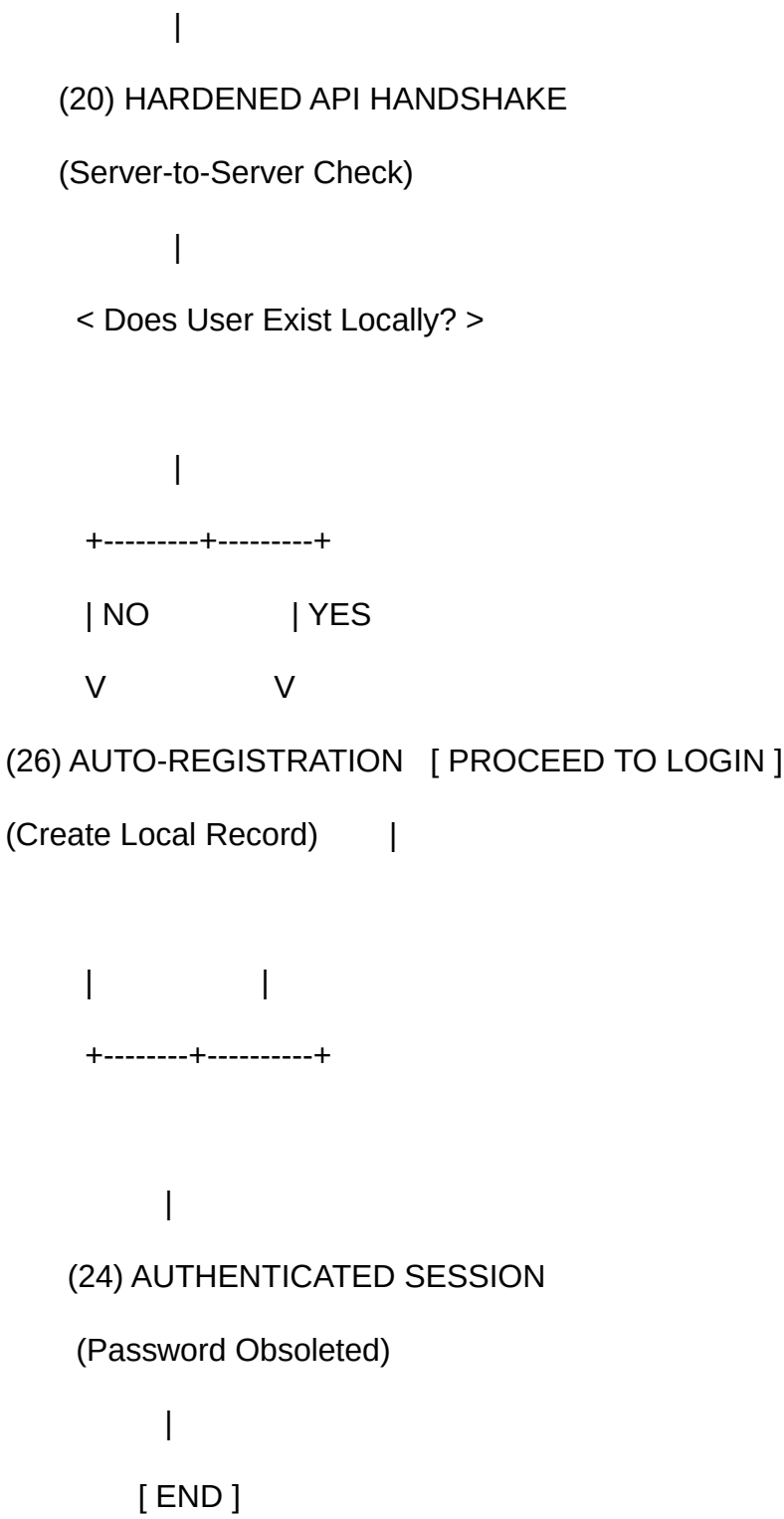
1. **User Device (10):** Client hardware, such as a smartphone or security key, equipped with a secure enclave and biometric sensors.
2. **Authentication Trigger (12):** The local user interaction (biometric scan or secure PIN) that unlocks the cryptographic hardware.

3. **Bridge Interface (14):** A client-side script injected into a Vendor Environment (22) that identifies legacy fields and redirects the user to the Centralized Vault (16).
4. **Centralized Vault (16):** The remote server (e.g., PHP 8.2) managing the JIT identity generation, vendor validation, and hardware-agnostic recovery logic.
5. **Cryptographic Proof (18):** A time-limited, single-use cryptographic token transmitted from the Centralized Vault (16) back to the Vendor Environment (22).
6. **Hardened API Handshake (20):** A server-to-server validation process where the Vendor Environment (22) sends the Cryptographic Proof (18) and a unique Vendor API Key to the Centralized Vault (16) for final confirmation.
7. **Vendor Environment (22):** The legacy server (e.g., PHP 5.6) which performs auto-provisioning of new users and session injection upon successful handshake validation.
8. **Authenticated Session (24):** The final state where the user is granted access to vendor assets without the requirement of a database-stored password.
9. **Auto-Provisioning Trigger (26):** A logic gate within the Vendor Environment (22) that automatically creates a local user record if the verified identity is unrecognized.
10. **Atomic Reset Flow (28):** A recovery path within the Centralized Vault (16) that permits the replacement of an obsolete hardware-bound credential with a new enrollment.

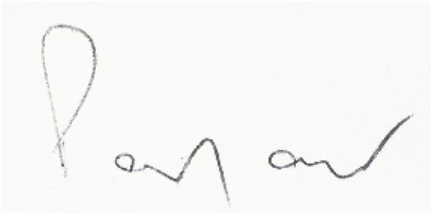
FIG. 1: Hardware-Backed Session Injection & Autonomous Identity Loop




[CENTRALIZED VAULT (16)] <----------+
(Generate Challenge)
|
(10) HARDWARE-BACKED UV
[BIOMETRIC] [SECURE PIN] [ERROR / NEW DEVICE]
(12a) (12b) (12c)
(28) ATOMIC RESET FLOW
(Delete Obsolete Cred)
[(10) SIGNATURE GENERATION] <---+ (Fresh Enrollment)
(Secure Enclave Release)
(18) CRYPTOGRAPHIC PROOF
(Single-use JIT Token)
[REDIRECT TO VENDOR]


(20) HARDENED API HANDSHAKE
(Server-to-Server Check)
< Does User Exist Locally? >
NO
YES
(26) AUTO-REGISTRATION
(Create Local Record)
[PROCEED TO LOGIN]
(24) AUTHENTICATED SESSION
(Password Obsoleted)
[END]

DATED AT BALLITO THIS 18TH DAY OF MARCH 2026.



Paul James Armer

RENEWAL SHEET

Year	Payment Date	Receipt Number	Amount

HISTORY SHEET

Date entry made	Description
2026-03-19	Request for the acceptance of a Patent electronically filed on 18/3/2026, numbered 2026/03023
2026-03-19	Proof reading performed automatically