PRVEN Human Authenticity Verification System

Technical Disclosure — Version 1.0

Author: Neal Robert Wright Drummond
Organization: PRVEN (Website: prven.org, Web app: identity.prven.org)
Publication Date: 12 March 2026

Important: Access Notice

---

1. Title

System and Method for Biometric Human Identity Verification, Cryptographic Identity Anchoring, and Public Authenticity Proof for Digital Identities

2. Publication Statement

This document constitutes a public technical disclosure describing systems and methods for verifying the authenticity of a human individual in digital environments through biometric verification and the generation of publicly verifiable authenticity records.

The purpose of this disclosure is to describe the underlying technical concepts, architectures, and operational methods in sufficient detail to place them into the public knowledge domain.

The systems and methods described herein may be implemented using a wide range of technical architectures, biometric modalities, infrastructure models, and deployment environments. The disclosure therefore describes a general framework for human authenticity verification and public verification signaling rather than a single implementation.

Publication Date: **12 March 2026**

---

3. Definitions and Terminology

For the purposes of this disclosure, the following terms may be used.

Human Verification

Human verification refers to a process in which a computing system determines that a real human individual is physically present during a verification event.

Human verification may involve biometric verification, liveness detection, behavioral analysis, sensor data analysis, or combinations of these techniques.

Liveness Detection

Liveness detection refers to techniques used to determine whether biometric input originates from a live human subject rather than from prerecorded media, synthetic media, or artificial representations.

Examples include motion analysis, facial movement detection, blink detection, challenge-response tasks, depth sensing, or machine learning classification.

Identity Anchor

An identity anchor refers to a persistent cryptographic or data representation that links a verification event to an identity reference representation.

Identity anchors may include:

- cryptographic hashes
- biometric templates
- digital identity tokens
- verifiable credentials
- cryptographic signatures

The identity anchor allows later verification of identity association without necessarily storing the original biometric data.

Verification Record

A verification record refers to structured data generated during a verification event describing the outcome of the verification process.

Verification records may include metadata such as:

- verification identifier
- timestamp
- verification method
- similarity scores
- confidence scores
- verification status

Public Authenticity Signal

A public authenticity signal refers to a publicly accessible representation of a verification record that allows third parties to confirm that a human verification event has occurred.

Public authenticity signals may include:

- public verification pages
- verification tokens
- QR codes
- API responses
- digital certificates

Likeness Usage Declaration

A likeness usage declaration refers to a public statement associated with a verified identity describing the permissions or restrictions regarding the use of the individual's likeness in artificial intelligence systems, synthetic media generation, or licensing contexts.

---

4. Background and Problem Space

Digital communication systems increasingly rely on representations of individuals such as profile photographs, videos, audio recordings, and other identity signals.

At the same time, advances in artificial intelligence and generative media technologies have enabled the creation of synthetic images, videos, and audio that can realistically mimic real individuals.

These technologies may be used to produce:

- deepfake videos

- synthetic voice recordings
- AI-generated avatars
- fabricated identity media
- impersonation content

As a result, it is increasingly difficult for third parties to determine whether a digital identity corresponds to a real human individual.

Existing verification systems used by online platforms typically rely on centralized platform-specific verification processes. These approaches often suffer from several limitations:

1. Verification status is limited to a single platform.
2. Verification records are not portable across services.
3. Verification signals cannot easily be verified independently.
4. Verification methods may require long-term storage of biometric data.
5. Individuals have limited ability to publicly assert authenticity outside of platform-controlled systems.

Additionally, there is currently no widely adopted mechanism through which individuals may publicly declare permissions regarding the use of their likeness in artificial intelligence systems.

The systems and methods disclosed herein address these problems by enabling:

- biometric human verification
- cryptographic identity anchoring
- generation of portable authenticity signals
- public verification of identity authenticity
- optional declarations regarding AI likeness permissions

---

5. Overview of the Concept

The disclosed system provides a framework for verifying that a real human individual corresponds to a digital identity and for generating a publicly verifiable authenticity record associated with that identity.

In general terms, the system operates through the following stages:

1. A user provides a reference identity representation.
2. The system performs biometric liveness verification using live capture.
3. The system compares live biometric input with the reference representation.
4. Verification metrics such as similarity and confidence scores are generated.
5. A cryptographic identity anchor is generated from the reference representation.
6. A verification record describing the verification event is created.
7. A public authenticity signal is generated and made accessible.

The public authenticity signal allows third parties to confirm that a human verification event occurred without requiring access to the original biometric inputs.

In some implementations the system may also store declarations describing how the verified individual authorizes or restricts the use of their likeness in artificial intelligence systems.

---

6. System Architecture

The disclosed system may be implemented using a variety of architectures. One example architecture is illustrated below.

User Device

Verification Interface

Biometric Capture System

In this architecture:

- the user device may capture biometric input
- the verification interface may guide the user through verification
- biometric verification services may perform liveness detection and identity comparison
- verification records may be generated and stored
- public verification interfaces may allow external verification

The architecture may operate using centralized, federated, or decentralized infrastructure.

---

7. System Components

The system may include several functional components.

Verification Interface

A verification interface may provide the user with the ability to initiate identity verification.

The interface may be implemented through:

- web applications
- mobile applications
- software development kits
- embedded identity verification modules
- third-party integrations

The interface may guide the user through reference identity submission and live verification.

Reference Identity Capture

The system may allow the user to provide a reference identity representation.

Examples include:

- facial photographs
- short video captures
- biometric scans
- device-captured identity signals

This representation serves as the baseline identity reference used during verification.

Biometric Liveness Verification

The system may perform liveness verification using one or more biometric signals.

Examples include:

- facial movement analysis

- blink detection
- motion verification
- challenge-response instructions
- depth sensing
- machine learning classification

The goal of liveness detection is to ensure that the biometric input originates from a real human individual during the verification event.

Biometric Comparison Engine

After liveness verification, the system may compare the captured biometric data with the reference identity representation.

The comparison may involve:

- facial feature vector comparison
- neural network embeddings
- biometric template matching
- probabilistic identity matching

The comparison may produce metrics including:

- similarity score
- confidence score
- verification probability

Verification Record Generator

If verification criteria are satisfied, the system generates a verification record.

The verification record may include:

- unique verification identifier
- timestamp
- geographic region
- similarity score
- confidence score
- verification status

This record represents the outcome of the verification event.

Identity Anchor Generator

The system may generate a cryptographic representation derived from the reference identity representation.

Examples include:

- cryptographic hashing
- digital identity signatures
- cryptographic fingerprints

This identity anchor allows the verification record to be associated with the identity reference without requiring storage of the original biometric media.

Public Verification Interface

A public verification interface may present verification information to third parties.

The interface may display information including:

- verification status
- timestamp
- verification region
- similarity score
- confidence score
- identity thumbnail representation
- likeness usage declarations

The interface may be accessible through a unique verification identifier.

Data Minimization Architecture

In some implementations the system may minimize storage of biometric media.

For example:

- full-resolution identity images may be deleted after verification
- cryptographic hashes may be retained
- low-resolution thumbnails may be retained

This architecture allows verification records to persist while reducing long-term biometric data storage.

---

8. Operational Verification Process

An example verification process may proceed as follows.

1. The user creates an account within the verification system.

2. The user submits a reference identity image.
3. The system requests live biometric capture.
4. Liveness detection verifies human presence.
5. The biometric comparison engine evaluates similarity.
6. Verification metrics are generated.
7. The system generates an identity anchor.
8. A verification record is created.
9. A public verification page is generated.

The verification page allows third parties to confirm the authenticity status of the identity.

---

9. Method for Generating a Public Human Verification Record

In some implementations the system may perform a method comprising the following steps:

1. receiving a reference identity representation associated with a user
2. capturing live biometric input from the user
3. performing liveness detection to confirm human presence
4. comparing the live biometric input to the reference representation
5. generating verification metrics including similarity scores
6. generating a cryptographic identity anchor derived from the reference representation
7. generating a structured verification record
8. storing the verification record within a verification registry

9. generating a publicly accessible authenticity signal associated with the verification record

This method may be implemented using a wide variety of biometric technologies, infrastructure models, and computing environments.

10. Privacy-Preserving Identity Verification Architecture

In some implementations, the disclosed system may be designed to reduce long-term storage of biometric media while still preserving verification records.

This may be accomplished by separating **biometric verification operations** from **long-term identity proof storage**.

In such architectures, biometric inputs may be used temporarily during verification and then removed once verification has been completed.

An example process may proceed as follows:

1. A reference identity representation is provided by the user.
2. The system performs biometric comparison and liveness verification.
3. Verification metrics are generated.
4. A cryptographic identity anchor is derived from the reference representation.
5. Verification metadata is stored.
6. Full-resolution biometric media may be deleted.

This approach enables identity authenticity verification while reducing the need for long-term storage of sensitive biometric data.

The retained verification artifacts may include:

- verification identifier

- verification timestamp
- similarity score
- confidence score
- verification status
- cryptographic identity hash
- optional thumbnail image
- likeness usage declarations

This architecture allows the system to function as a **verification registry without maintaining biometric databases**.

In some implementations, low-resolution images or thumbnails may be retained for display purposes while full-resolution biometric inputs are removed.

---

11. Registry-Based Human Verification Systems

In some implementations, verification records may be stored within a registry that contains records describing completed human verification events.

Such registries may function as repositories of verification records associated with verified identities.

A verification registry may store entries including:

- verification identifier
- identity anchor
- verification timestamp
- verification method information

- verification scores
- verification status

Registries may be implemented in a variety of ways including:

- centralized database systems
- distributed data storage systems
- federated identity verification systems
- decentralized identity networks
- blockchain-anchored registries

In some implementations the registry may only be accessible through unique verification identifiers.

In other implementations the registry may support query interfaces or APIs that allow systems to confirm verification status.

Registries may function as a **public trust signal infrastructure** that allows third parties to verify whether an identity has previously completed a biometric human verification process.

---

12. Likeness Usage Declaration Framework

The system may allow verified individuals to publish declarations regarding how their likeness may be used in artificial intelligence systems or synthetic media generation.

Such declarations may include statements such as:

- prohibition of AI training usage
- conditional licensing permissions
- licensing available upon request

- open licensing permissions

These declarations may be stored alongside verification records or associated with the identity anchor.

In some implementations these declarations may function as **public notices of likeness rights**.

Third-party systems may reference these declarations when determining whether an individual's likeness may be used within:

- training datasets
- generative media systems
- synthetic content generation tools
- licensing marketplaces

The declarations may also include optional contact information through which licensing requests may be submitted.

---

13. Variations and Alternative Implementations

The systems described in this disclosure may be implemented using many different technologies and configurations.

The disclosed concept is not limited to any specific biometric modality or verification infrastructure.

Examples of biometric verification signals include:

- facial recognition
- voice recognition
- iris scanning

- fingerprint scanning
- gait recognition
- behavioral biometric signals

Verification may involve one or more biometric modalities simultaneously.

Biometric comparison may be performed using:

- neural network embedding comparison
- feature vector similarity measurement
- probabilistic matching algorithms
- rule-based biometric verification

Identity anchors may be generated using different cryptographic techniques including:

- SHA family hashing algorithms
- cryptographic fingerprinting
- Merkle tree commitments
- blockchain transactions
- digital signature systems

Public authenticity signals may take many forms including:

- web-based verification pages
- machine-readable verification APIs
- digital certificates
- verification badges
- QR code verification tokens

The verification system may be integrated into:

- social media platforms
- identity wallets
- creator platforms
- messaging platforms
- authentication services

The disclosed system may therefore operate as a **general human authenticity verification infrastructure** across many digital environments.

---

14. Deployment Architectures

The disclosed system may be deployed in multiple infrastructure configurations.

Centralized Systems

In centralized implementations, verification services may operate on centralized server infrastructure.

Biometric verification, verification record generation, and identity anchor storage may all occur within a cloud-hosted system.

Federated Identity Systems

In federated implementations, multiple verification authorities may operate within a shared identity verification ecosystem.

Each authority may perform biometric verification independently while contributing verification records to a shared registry.

Decentralized Identity Systems

In decentralized architectures, verification records or identity anchors may be anchored to distributed networks such as blockchain systems.

In such implementations, verification records may be published as cryptographic commitments within decentralized identity networks.

Device-Based Verification

In some implementations biometric verification operations may occur locally on user devices.

Mobile devices or secure hardware modules may perform biometric verification and generate signed identity verification tokens.

---

15. Example Implementation

One example implementation of the disclosed system may operate as follows.

A user creates an account within an identity verification platform.

The user uploads a reference facial image.

The system requests a live liveness capture from the user through the user’s device camera.

The captured live input is evaluated using liveness detection algorithms to confirm that a real human is present.

The system compares the captured biometric input to the reference representation using facial comparison algorithms.

If the similarity score exceeds a defined verification threshold, the system records a successful verification event.

The system generates a cryptographic hash derived from the reference identity representation.

A verification record is created containing:

- verification identifier
- verification timestamp

- verification region
- similarity score
- confidence score
- verification status

The verification record is stored within a verification database.

A public verification page associated with the verification identifier is generated.

The page may display verification status and selected verification metadata.

The full-resolution reference image may then be removed from storage while retaining a thumbnail representation and cryptographic identity anchor.

---

16. Additional Embodiments and Extensions

The disclosed system may support a wide range of additional features and extensions.

Examples include:

- automated impersonation detection systems
- monitoring for synthetic media misuse
- identity authenticity verification APIs
- browser extensions that confirm identity authenticity
- digital content authenticity indicators
- licensing systems for biometric likeness rights
- integration with digital identity wallets
- automated verification status badges

Future implementations may integrate the verification system with identity infrastructure used by:

- creator platforms
- financial services
- digital marketplaces
- social media systems
- content distribution platforms

---

17. Use Cases and Applications

The disclosed system may be applied in many different contexts.

Examples include:

Creator Identity Verification

Online creators may use the system to publicly prove that they correspond to a real human individual.

Public Figure Authenticity

Public figures may use verification records to demonstrate that official content originates from verified human identities.

Deepfake and Impersonation Mitigation

Verification signals may help audiences determine whether media originates from verified individuals.

Digital Trust Systems

Platforms may use verification signals to establish trust in digital identity representations.

Identity Infrastructure

The system may function as a general infrastructure layer for confirming human authenticity across digital services.

---

18. Summary

The systems and methods disclosed in this document describe a framework for verifying that a real human individual corresponds to a digital identity and for generating publicly verifiable authenticity records.

The system combines biometric human verification, cryptographic identity anchoring, and public authenticity signaling to create portable identity verification records.

By separating biometric verification from long-term biometric storage and by publishing verification records as authenticity signals, the system allows third parties to verify identity authenticity while reducing privacy risks associated with storing biometric datasets.

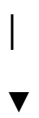
The disclosed architecture may be implemented using a wide range of biometric technologies, infrastructure models, and deployment environments.

Accordingly, the disclosure describes a broad framework for **human authenticity verification and public identity proof generation** that may be applied across many digital systems.

---

19. System Architecture Diagram

User Device



Verification Interface

▼

Reference Identity Capture

|

▼

Liveness Detection Engine

|

▼

Biometric Comparison Engine

|

▼

Verification Record Generator

|

▼

Identity Anchor Generator

|

▼

Verification Record Storage

|

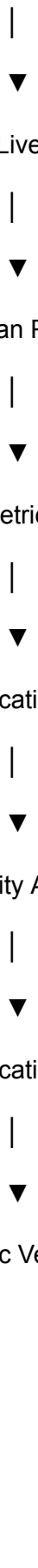
▼

Public Verification Interface

---

20. Verification Process Flow Diagram

User Uploads Reference Identity


Live Liveness Capture
Human Presence Verification
Biometric Identity Comparison
Verification Score Generation
Identity Anchor Generation
Verification Record Creation
Public Verification Page Generation