

SENSECRYPT

Cutting edge, privacy-focused identity
and security technology



SEVENTH
SENSE

DIGITAL IDENTITY CHALLENGE



Growing Threats Outpace Traditional Authentication Methods

Traditional authentication methods, primarily relying on passwords and tokens, are increasingly vulnerable to sophisticated cyber threats like phishing, social engineering, and brute-force attacks, making these methods insufficient for current security demands.



Conventional Biometric Systems Store Biometric Data

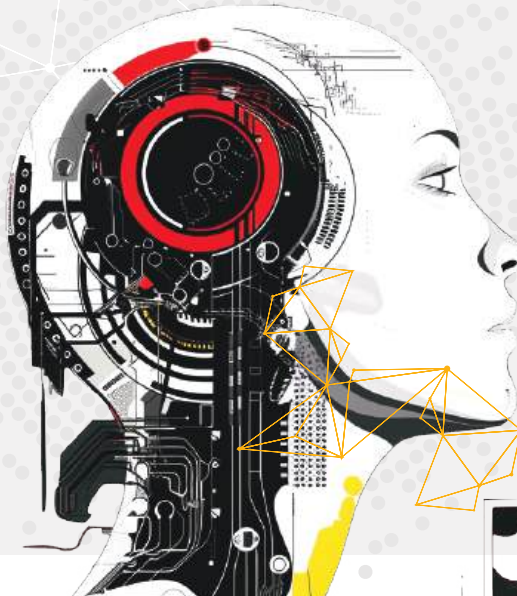
Biometric authentication leverages unique physiological characteristics such as fingerprints and facial features for identification. While offering enhanced security, traditional biometric systems require storing sensitive biometric data, raising significant privacy concerns. Data breaches involving biometric information are particularly damaging since biometric traits cannot be changed like passwords.



Quantum Algorithms Break Widely Used Cryptographic Methods

Quantum computing poses a significant threat to existing cryptographic systems like RSA and ECC. Quantum algorithms could potentially break these widely used methods, compromising the security of encrypted data and communications. This necessitates a transition to quantum-resistant cryptographic algorithms to ensure long-term data protection.

Thus, the evolving digital landscape requires a balanced approach, where biometric technologies must evolve in tandem with technological advancements, regulations, emphasizing user rights, transparency, and accountability.



INTRODUCING SENSECRYPT

Seventh Sense addresses these multifaceted issues by combining biometric authentication with advanced cryptographic techniques, including post-quantum cryptography through its patent-pending SenseCrypt technology solution (SenseCrypt).

SenseCrypt eID & SensePrints

At the heart of the platform is the innovative SenseCrypt eID, which generates SensePrints – encrypted, compact data structures that serve as Verifiable Credentials. These SensePrints contain no biometric data but can be verified using the eID holder's face. Their small size (~ 350 bytes) allows for easy storage and transmission, enabling storage in NFC chips, databases or representation as QR codes.

Face-Based Public Key Infrastructure

SenseCrypt introduces the world's first Face-based Public Key Infrastructure (Face PKI). This system enables the creation of Face Certificates, which are Verifiable Presentations – standard X.509v3 certificates with face-derived public keys. These certificates allow for secure transactions without the verifier ever seeing or processing the eID user's face. The integration of post-quantum cryptography further enhances the security of Face Certificates.

Distributed Ledger Technology Protocol

This innovative protocol brings biometric verification to Distributed Ledger Technology (DLT) without storing or transferring biometric data. It solves the challenge of trusting digital wallets in blockchain applications by using a Trusted Witness system and Witnessed Credentials.

Face-Based mTLS Protocol

The Face-Based mutual Transport Layer Security (mTLS) Protocol aims to secure internet connections at the transport layer using face-based authentication. This innovation has the potential to eliminate the need for traditional authentication methods like usernames, passwords, and One-Time Passwords (OTPs).



PRIVACY BY DESIGN

Privacy is a fundamental right. SenseCrypt's revolutionary technological breakthrough enables privacy-focused facial verification without storing any biometric data or facial images anywhere. This GDPR-compliant technology puts users in control of their identity and data, eliminating privacy risks and ensuring complete security.

SenseCrypt eID: 0% Biometrics, 100% Privacy

SenseCrypt eID is a groundbreaking privacy-preserving biometric identity solution.

A core feature of SenseCrypt eID, Zero-Knowledge Face Proofs, enables face verification without revealing or storing biometric data. This innovation transforms face recognition from a machine learning challenge into a cryptographic solution, creating tokenized biometrics. Through zero-knowledge proofs, verifiers can authenticate users without ever accessing or processing their biometric data, ensuring full compliance with GDPR's "data protection by design and by default." The system delivers robust authentication and verification without requiring internet connectivity or storing facial templates, providing unparalleled security and reliability

Broad Use Cases

SenseCrypt eID



Proof of
Personhood



Biometric ID

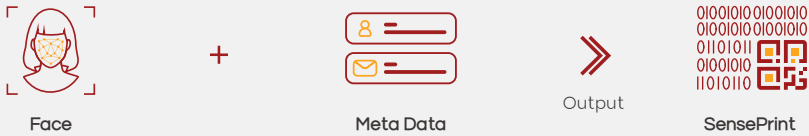


Identity Verification
& Authentication



Access
Control

Registration



Devoid of any biometric data in any form, SensePrints provide the basis for secure and privacy-centric digital identities, delivering an essential balance between security, privacy, and convenience.

Authentication



For verification, the person is authenticated if their face generates the correct private key and successfully decrypts the SensePrint.

How it works

SensePrints are generated from a person's face (optionally combined with metadata or a password) to create an encrypted, privacy-preserving binary data structure. This structure is approximately five times smaller than traditional biometric templates and acts as a secure identity marker without storing actual biometric data. This approach revolutionizes identity verification by enhancing security and privacy, transforming the way identity verification is conducted.

Rather than relying on traditional methods of storing and matching biometrics, SenseCrypt eID employs encryption for registration and decryption for authentication, without storing any public or private keys.

SensePrints can be printed as QR codes on IDs or stored in NFC chips and databases. SensePrints can be verified offline with ease.

TRADITIONAL FR

In traditional FR a template is like a key.

Registration



generates



a Key

which is



stored in a database.

Verification



New Key

And compared with



Stored Key

Similar enough?
Yes = Verification

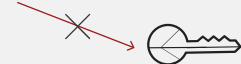
Properties

Reversible



Template can be reversed into a face

Non-Revocable & Non-Renewable



No new template can be generated from the same image

Linkable



Database A



Key



Linkable



Key



Database B

Template can be compared across databases and linked as belonging to the same person

vs. SENSECRYPT

In contrast, a SensePrint is like a Locked Safe.

Registration



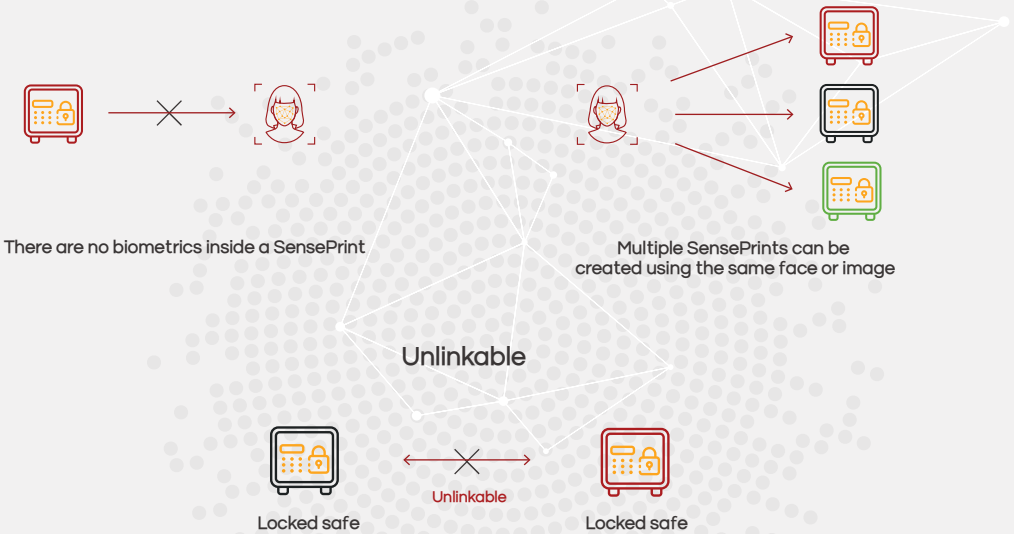
Verification



Properties

Irreversible

Revocable & Renewable



Unlinkable



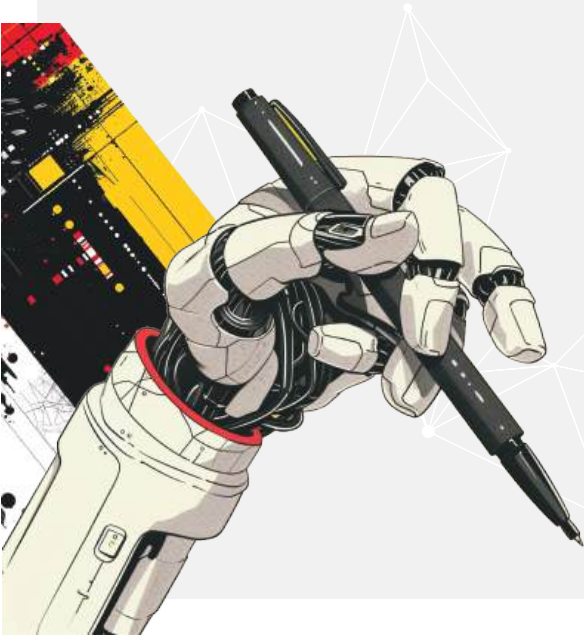
By comparing two SensePrints it is not possible to say if they belong to the same person or two different people

SenseCrypt eID Privacy Advantage

Storing biometric data poses significant privacy risks. If biometric databases are breached, the compromised data cannot be changed like a password, leading to permanent security issues for affected individuals. For instance, a breached biometric database allows linking an individual across different systems.

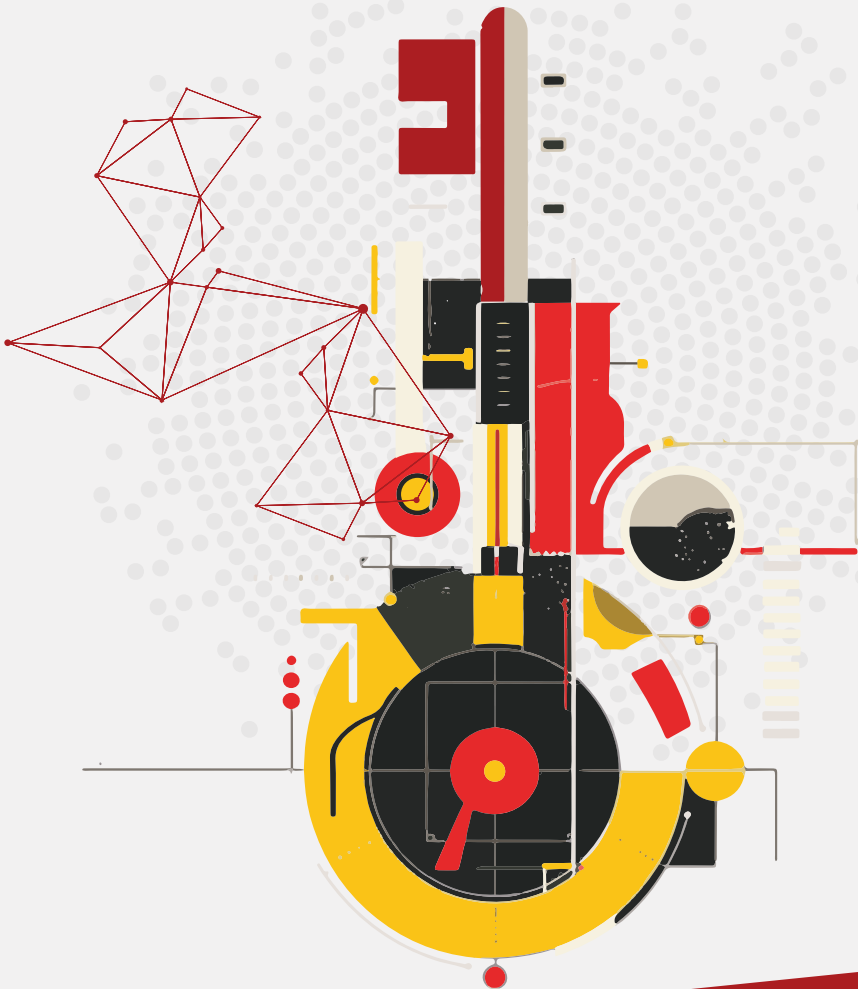
SenseCrypt eID eliminates the need to store any biometric data, addressing privacy concerns directly. By transforming biometric authentication into a cryptographic process, it ensures:

- **Data Minimization:** Only essential data is used for authentication, and none is retained after the process.
- **Reduced Attack Surface:** With no biometric data stored, there is no centralized repository for attackers to target.
- **Enhanced User Trust:** Users can be confident that their sensitive biometric information is not at risk.
- **Reduced Compliance:** By eliminating the need to store biometric data, SenseCrypt simplifies compliance with data protection regulations like GDPR and CCPA. Organizations can adopt SenseCrypt eID without the extensive regulatory burdens associated with handling sensitive personal information. Even if the issuer and verifier encryption keys are compromised, there is zero access to personally identifiable information (PII).



THE ACE IN FACE

While SenseCrypt eID requires the user's live face for each transaction, with authentication through the decryption of the SensePrint, SenseCrypt's Face PKI utilizes the construct of the well-established and accepted PKI framework and employs a unique and proprietary approach of face-derived cryptographic key pairs. Face PKI enables secure verification and transaction signing without the verifier ever needing to see the user's face – a breakthrough that sets it apart.



Introducing Face-Based PKI: Unlock the future

This world-first Face-based Public Key Infrastructure allows the creation of Face Certificates, which are Verifiable Presentations.



Face

+



SensePrint



Output



How it works

Public Key for specified purpose:
Z3VydQ==
(Face-derived Public Key)

Requested eID attributes
Name, Address, DOB

Expiry Date
7/7/2077

Expiry Certificate Revocation List
<https://mycrl.com>

Signature by foundational eID issuer
aXNzdWVy

Face Certificates are generated using the user's face and their SensePrint eID. As in traditional PKI, a **face-derived public key** is embedded in the digital certificate, which can be used for authentication, encryption, and secure signing. The PKI trust hierarchy and certificate authorities are used to establish trust within the system, just as in a traditional PKI system.

Face Certificates are standard X.509v3 certificates, but instead of certifying websites, Face Certificates certify individuals and enable transactions using their face without requiring access to or processing of any facial or biometric data.



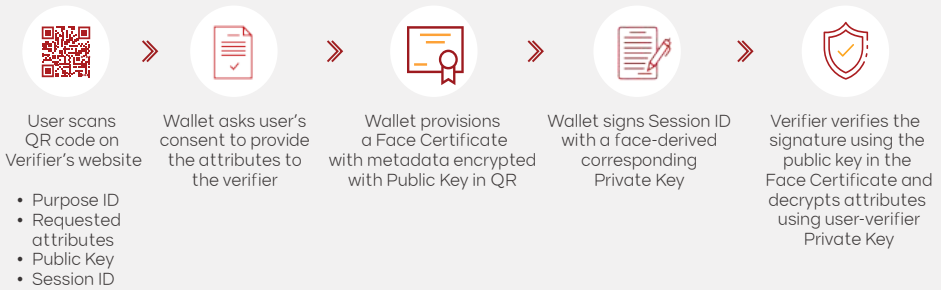
The Benefits

- **Revocable and renewable** using standardized constructs (Certificate Revocation List) **Issue and revoke your digital identity and keys instantly on-demand**
- Have a **configurable expiry date**
- **Uses familiar technology** without requiring deployment of a distributed technology such as blockchain
- **Provides privacy** (use of pairwise functional eID) while still allowing for some centralization and control by a foundational eID organization
- **Unlock use cases beyond identity** – Login, Signing, Encryption / Decryption

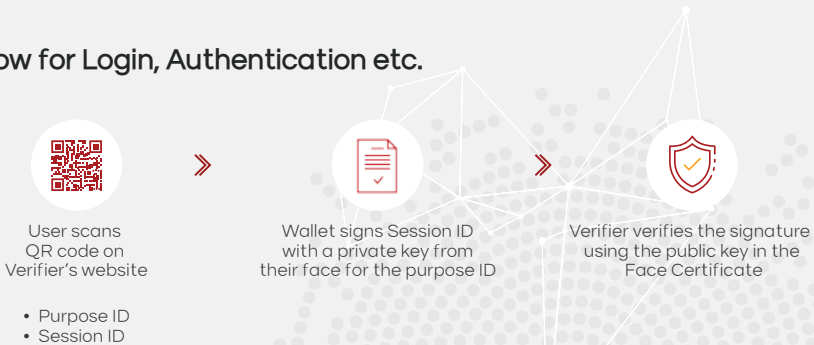
Broad Use Cases



User Flow for eKYC, Face Certificate Generation



User Flow for Login, Authentication etc.



Post-Quantum Cryptography: Futureproofing

The integration of Post-Quantum Cryptography (PQC) is a unique and critical feature that future-proofs SenseCrypt platform. By implementing PQC, Seventh Sense addresses a critical vulnerability in current cryptographic systems. Many of today's encryption methods, particularly those based on factoring large numbers or solving discrete logarithm problems, are vulnerable to attacks by large-scale quantum computers. Quantum algorithms like Shor's algorithm could potentially break these cryptographic systems, posing a significant threat to data security and privacy.

The platform adopts the quantum-resistant algorithms selected by the National Institute of Standards and Technology (NIST). Specifically, Face PKI implements:




CRYSTALS-KYBER: A module-lattice-based key encapsulation mechanism, designed to resist attacks from both classical and quantum computers, providing secure key exchange for encrypted communications.

CRYSTALS-DILITHIUM: A module-lattice-based digital signature algorithm, ensuring the integrity and authenticity of digital signatures in a post-quantum environment.

SPHINCS+: A stateless hash-based digital signature algorithm, providing an additional layer of post-quantum security for digital signatures.

In line with the recommendations from the European Union Agency for Cybersecurity (ENISA), Face PKI also supports a hybrid approach to cryptographic agility by integrating traditional cryptographic algorithms with post-quantum algorithms.

The adoption of PQC standards allows Face PKI to offer:

-  **Long-Term Security:** Data encrypted today will remain secure even if powerful quantum computers become available in the future.
-  **Compatibility with Existing Systems:** The PQC algorithms are designed to work within current cryptographic frameworks, allowing for smoother integration and transition.
-  **Resistance to Both Classical and Quantum Attacks:** The chosen algorithms provide protection against both traditional and quantum-based cryptanalysis.



Face-based mTLS Protocol: Security at Transport Layer

Forget about usernames, passwords, and OTPs. In the future, your internet connection could be encrypted with your face! And that too at the most fundamental layer – the Transport Layer.

The Face-Based Mutual Transport Layer Security (mTLS) Protocol is an innovative approach to securing internet connections through face-based authentication. Traditionally, in mutual TLS (mTLS) protocols, a server verifies a client's certificate via a CertificateVerify message during the TLS handshake. This message includes a signature of all preceding handshake messages, signed using the private key linked to the client's certificate.

In the Face-Based mTLS Protocol, the client certificate is replaced with a Face Certificate. To perform a mutual TLS handshake, the client must generate a private key that can only be created using the face of the Face Certificate holder. This unique key is then used to sign the CertificateVerify message.

By securing all applications, browsers, and other connections to the server with facial authentication, this protocol ensures that websites and companies are interacting with a live human rather than a bot or AI agent. This secure technology places humans at the center, enabling them to better control and trust their online experiences without sacrificing privacy.

Potential Advantages

- **Eliminates Traditional Credentials:** Could replace usernames, passwords, and OTPs, simplifying the authentication process.
- **Integrated Security:** Embeds biometric authentication directly into the mTLS handshake at the transport layer.
- **Strong Protection:** Enhances security against man-in-the-middle attacks and unauthorized access.

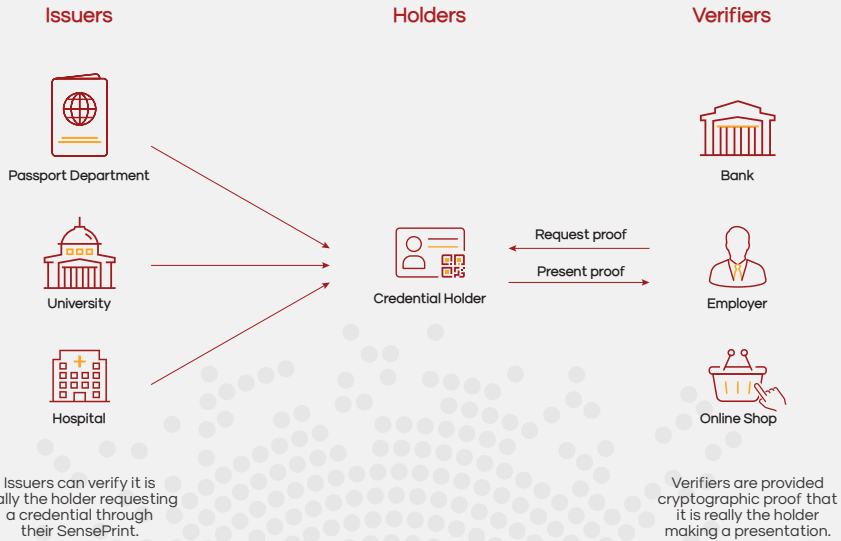


YOU PROVE YOU

SenseCrypt DLT Protocol: Trust the Wallet – Bringing Biometric Trust to Blockchain Without Storing or Transferring Biometrics

Store your Verifiable Credentials securely in an identity wallet and present them easily as a Verifiable Presentation whenever needed. SenseCrypt DLT enhances this process with Face Verified Credentials and Face Attested Presentations. Credentials are granted only after face verification—without storage, transmission or processing any biometric data. Verifiers receive cryptographic proof confirming that you are the one performing the transaction





Features of your Private Digital ID

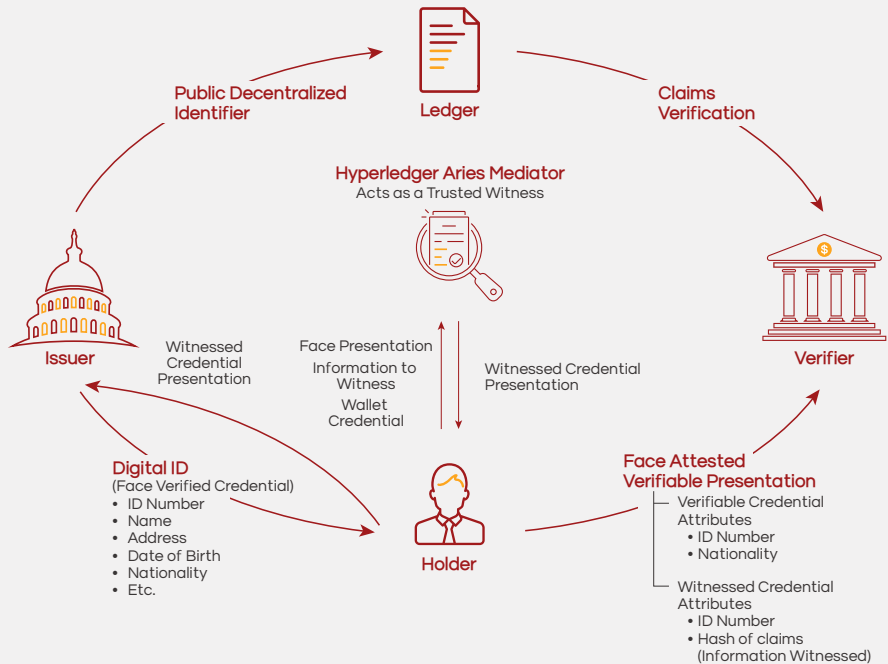
- **Biometrics Attested Verifiable Presentations:** Maintain privacy with a Trusted Witness issuing Witnessed Credentials, ensuring Holder Binding in decentralized domains.
- **Non-Correlatability:** Privacy remains intact without compromising security, as data can't be traced back to an individual with the use of a Trusted Witness.

Broad Use Cases

SenseCrypt DTL Protocol



Our Solution



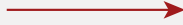
Simplified Flow

1. The central piece in the SenseCrypt DLT Protocol is a Hyper Ledger Aries Cloud wallet which is configured to act as a Trusted Witness.
2. Upon wallet activation, the wallet provides the Trusted Witness a Face Presentation and gets back a Wallet Credential containing a SensePrint. This invisible credential lives in the user's wallet and binds the wallet to the user's face.
3. Subsequently the Trusted Witness is also capable of receiving a presentation of a Wallet Credential issued earlier, a Face Presentation and a hash of Information to Witness.
4. Upon receiving the above, the Trusted Witness issues a transactional Witnessed Credential containing a **new SensePrint** and the hash of Information to Witness.
5. A presentation of the Witnessed Credential is required for each transaction whether it is the issuance of a new credential or the verification of an existing credential's presentation. Since the Witnessed Credential contains a **new SensePrint** for each transaction, it avoids the problem of linkability, and of storing biometrics in credentials.

User Journey – Issuance



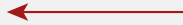
Issuer generates connection invitation QR code



Holder scans QR code on Issuer's website using their wallet



Issuer verifies SensePrint in Witnessed Credential against the Holder's face and Wallet gets a Face Verified Credential.



Wallet gets a Witnessed Credential from the Trusted Witness using the Holder's face scan and presents it to the Issuer.

User Journey – Verification



Holder Scans connection invitation QR code on the Verifier's site



Wallet Requests a Face Scan from the Holder for creation of a Face Attested Presentation



Face Attested Claims are received and verified



Wallet creates a Face Attested Presentation of requested claims



DIFFERENCE, SPOTTED.

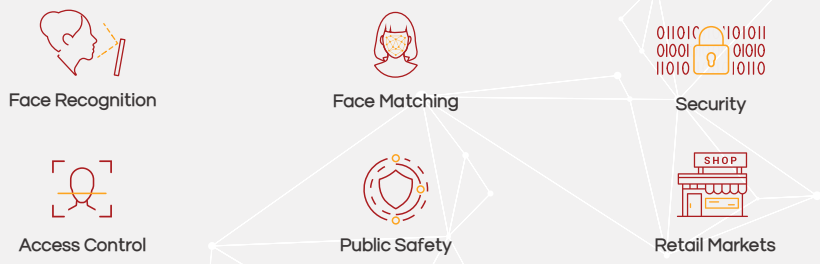
OpenCV FR: Ranked among the top 10 algorithms globally by NIST.

Trusted by OpenCV, experience easy, accurate, and secure face recognition as the new standard.

Discover scalable face recognition

We have partnered with OpenCV, the leading Computer Vision library, to deliver top-tier Face Recognition technology. Our API-based solution offers easy-to-use, scalable, and secure Face Recognition as a service, deployable on any internet-connected device. Utilizing deep learning, our technology accurately detects, recognizes, and compares faces, enabling applications such as one-to-many face search, face comparison, access control, attendance management, etc.

Smart vision for a smarter future



Liveness/Anti-Spoofing

Our solutions feature cutting-edge liveness and anti-spoofing detection to ensure security. This technology detects presentation attacks with just one image, enhancing the user experience while maintaining high-security. Our liveness feature meets ISO 30107 Level 1/Level 2 standards with a 0% error rate.

NIST Twins Analysis

We excel in the NIST Twin Analysis, demonstrating exceptional performance in False Match Rate (FMR) evaluations, even when comparing twins.

Racial Bias Assessment

We ensure minimal racial bias by analyzing variance across diverse countries, demonstrating our commitment to fairness.

Edge FR & Machine Vision (Partner Solutions)

Partner with us and industry leaders like Intel, Blaize, and SophGo for Edge FR and Machine Vision solutions tailored to your needs.

On-Premises Server

Our On-Premises Server solution provides the same features as our web API, but with the added benefit of being deployable on your own servers for enhanced data security and compliance with internal policies.



Certified by



What shapes our story

At Seventh Sense, our logo represents more than just a symbol — it is a reflection of our unwavering commitment to security and safety. Inspired by the ancient rune **Algiz**, historically associated with protection, our emblem reflects our core values of security, trust, and reliability. In an era where digital threats are pervasive, we view our logo as a shield against breaches. Our mission is clear: to deliver cutting-edge AI solutions that keep individuals, organizations, and nations safe.

**SEVENTH
SENSE**

Seventh Sense Artificial Intelligence Private Limited.
101 Cecil Street #11-01, Singapore 069533.
www.seventhense.ai