SENSECRYPT

A person-bound root of trust.
Identity, access, signatures and AI-agent authority tied to a live person.



SEVENTH SENSE

WHAT SHAPES OUR STORY

A symbol of protection.

At Seventh Sense, our logo is more than a symbol. Inspired by the ancient rune **Algiz**, long associated with protection, it reflects our core values of security, trust and reliability.

In an era of pervasive digital threats and autonomous AI, we build identity technology that ties credentials, signatures, sign-in and AI-agent authority to a live person, without storing the things attackers want.

We are a Singapore-based deep-tech company. Our founders previously built a mobile security company that was acquired by Intel/McAfee.

Some of our notable investors include Singapore's Ministry of Defense, and government entities from Singapore and Australia.

WHAT WE BUILD ON

Open standards. Enterprise-ready.

SenseCrypt plugs into the identity standards your systems already use, so there's nothing to rip and replace.

STANDARDS	OIDC / OAuth 2.0 · PKCE · PAR · SAML 2.0 · SCIM 2.0 · CIBA · FAPI 2.0 · FAPI-CIBA · Strong client auth · M2M
ENTERPRISE	Multi-tenant · RBAC · Tamper-evident audit

WHAT WE BELIEVE

Identity systems fail because something valuable sits in storage.

So we built one with zero biometric storage, where PKI private keys never exist at rest.

At its heart is a quantum-safe, sealed, biometric-free, disposable face token per enrolled user: rotating, single-use, and containing no PII.

Identity fails where something valuable is stored.

Passwords, biometric databases and private-key files share one weakness: they exist at rest, waiting to be copied. Four pressures now make that weakness urgent.

01 Stored secrets get phished

Passwords, one-time codes and bearer tokens can be phished, replayed or stolen at scale. A credential that exists in storage is a credential that can be copied.

02 Biometric databases are honeypots

Conventional biometric systems retain face images or templates. A breached template cannot be reset like a password, and it can be used to link one person across systems.

03 Quantum puts today's keys on a clock

Identity credentials issued today need protection that lasts into the post-quantum era. NIST has standardized ML-KEM (FIPS 203) and ML-DSA (FIPS 204) for that transition.

04 AI agents act without a face

Autonomous agents now sign in, call tools and move data on our behalf. Every autonomous agent should be accountable to a verified human.





INTRODUCING **SENSECRYPT**

A person-bound root of trust.

SenseCrypt ties credentials, access, signatures, sign-in and AI-agent authority to a live person. Its core turns a live face into a quantum-safe, sealed, biometric-free, disposable face token: rotating, single-use, and containing no PII. In SenseCrypt PKI, it generates post-quantum private keys in memory for each operation, then discards them.

Zero biometric storage. PKI private keys that never exist at rest. Quantum-safe.

≥256 BITS
Residual entropy, by design

IdP APP ACCESS	LAUNCHED	Passwordless sign-in by live face check over OIDC, SAML 2.0 and SCIM 2.0.
eID CREDENTIALS	AVAILABLE	Digital credentials verified against their holder, even offline from a printed QR.
PKI SIGNING	AVAILABLE	Post-quantum signing and decryption keys generated by your live biometric.
ZKP DISCLOSURE	DESIGN PARTNERSHIPS	Prove the one fact a service needs. Withhold the rest.
KYA AI AGENTS	EARLY ACCESS	Know Your Agent: trace every AI agent's authority to a verified human.

HOW **SENSECRYPT** WORKS

Our face token. A locked safe, not a key.

> A quantum-safe, sealed, biometric-free, disposable face token per enrolled user: rotating, single-use, and containing no PII.

SenseCrypt never stores a face or a template.

REGISTRATION

The live face generates a quantum-safe, sealed face token.



VERIFICATION

A live face regenerates the key to unseal the token, thus verifying the person.

Quantum-safe

Sealed with symmetric and hash cryptography only: AES-256-GCM, HKDF-SHA256 and SHA-256.

Biometric-free and irreversible

No biometric inside; engineered so it cannot be reversed into a face.

Rotating and single-use

Each face token is disposable and replaced as it is used.

Unlinkable

Designed so two face tokens cannot be matched to the same person by default.

Revocable and renewable

Revoke a face token and issue a fresh one from the same face or image.

No PII

The face token carries no personally identifiable information.

ARCHITECTURE

Three steps. One human.

One credential. Two outputs: zero-knowledge proofs or cryptographic signatures.

ISSUANCE 01

Bind a credential to a human.

eID

RECOVERY GATE 02

A live, verified human unlocks the credential.

OPERATIONS 03

Two branches: proofs or keys.

ZKP PKI

THE TECHNOLOGY

Four disciplines. One construction.

ML Machine learning

A high-dimensional random projection of the face embedding separates genuine and impostor margins by design.

PQC Post-quantum crypto

ML-DSA signatures and ML-KEM key encapsulation in SenseCrypt PKI.

ZK Zero-knowledge proofs

STARK-based proofs with a transparent setup, with no trusted ceremony to compromise. Used in SenseCrypt ZKP.

ECC Error correction

Confidence-weighted, soft-decision decoding tolerates natural variation between two captures of the same face.

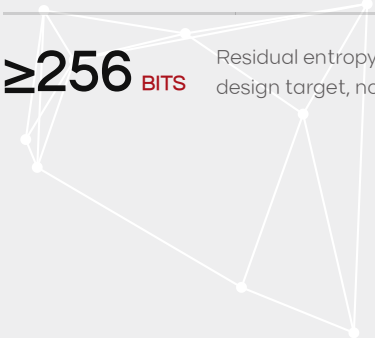
A key your face generates. Never saved.

CAPTURE	GENERATE	USE	DISCARD
Live face, checked by presentation-attack detection	Key pair generated in memory	Face sign or face decapsulate	Private key gone; public key stays

USE	ALGORITHM	STANDARD
PKI signatures	ML-DSA	FIPS 204
PKI key encapsulation	ML-KEM	FIPS 203
PKI classical option	secp256k1	ECDSA · classical option
Face token	AES-256-GCM	HKDF-SHA256, SHA-256 · symmetric & hash only
IdP federation	ES256 / RSA	Classical · OIDC / SAML
Transport	X25519MLKEM768	Hybrid post-quantum TLS, where negotiated

≥256 BITS

Residual entropy: the target for a quantum-safe construction. This is a design target, not a measurement or NIST certification.



SENSECRYPT IDP LAUNCHED

Sign in by face. No passwords.

SenseCrypt IdP is privacy-preserving biometric authentication that stores no biometric templates or images. People sign in to websites, applications and high-security platforms simply by using their face, including environments that require Financial-grade API (FAPI) 2.0 and strong client authentication.

Plug and play

Built on industry standards. Low-code or no-code integration with your existing identity infrastructure, with no rip and replace.

Nothing to phish

Passwords can be stolen, phished, forgotten or compromised. IdP removes them from sign-in.

Lower cost, better experience

Fewer password-related helpdesk requests and lower operating costs, with faster sign-in for users.

Three login methods. One identity layer.

01 Simple QR: scan an on-screen code and complete the face match on your own enrolled phone.

02 Passkeys+: FIDO2/WebAuthn passkeys plus a live face proof, phishing-resistant through origin binding.

03 Simple Webcam: enterprise and deviceless, with no phone needed. Licensed on-premises, on secure terminals.

OIDC / OAuth 2.0 · PKCE · PAR · SAML 2.0 · SCIM 2.0 · CIBA · FAPI 2.0 · FAPI-CIBA · Strong client auth · M2M · Multi-tenant · RBAC · Tamper-evident audit

Hosted or on-premises. Provision users from existing photos. Session persistence is configurable per tenant.



SENSECRYPT EID AVAILABLE

Verify the holder. Even from a printed QR.

SenseCrypt eID issues verifiable electronic identity without building the thing every adversary wants: a biometric database. No biometric images. No template database. Only a sealed, biometric-free face token.

Wallet, server, blockchain, or paper

In a wallet: on the holder's own device, presented on demand.

On a server: held in program infrastructure.

On a blockchain: anchored on a ledger.

As a printed QR: fully offline, for borders, aircraft and remote checkpoints.

> Sovereign by architecture: verification needs no connection to Seventh Sense.

How a verification works

Present

The holder presents the credential in any format.

Capture

Presentation-attack detection confirms a live human.

Recreate

The face unseals the face token and recreates the never-stored key.

Discard

The key is discarded. Offline, no capture leaves the verifier.

Offline checks require a prepared, supported verifier and trusted issuer material; revocation freshness depends on the verifier's update policy.

SENSECRYPT PKI AVAILABLE

Post-quantum keys. Generated by your live biometric.

Sign and decapsulate with post-quantum keys generated from your live biometric. Public keys are stored; private keys never are.

Face sign

Produces an ML-DSA signature that anyone holding the public key can verify with standard libraries.

Face decapsulate

Encapsulate to the stored ML-KEM public key; the live face generates the private key only to decapsulate.

Signing tied to human presence

The private key is generated from a live face check at the moment of signing, from a construction with ≥256 bits of residual entropy. Applications bind the signed data to the intended approval or document.

Certificates and CA custody

Face certificates work within a standard PKI. A split-verification design separates roles in establishing the person's certificate. Protected by our Face PKI patent (page 13).

Use cases

Document signing | Transaction approval | Encryption & decryption | Step-up authentication

SENSECRYPT ZKP DESIGN PARTNERSHIPS

Share the fact. Keep the rest private.

Zero-knowledge credentials that prove a live biometric match and disclose only the single fact a verifier needs: “over 18,” not a birthdate; “licensed,” not a license number.

Answer the question. Withhold the document.

Age thresholds without birthdates, residency without addresses, entitlement without enrollment history.

Verify the match, not the biometric

The verifier learns that the live face matched the credential’s face token, and nothing about the biometric itself.

Unlinkable by default

Proofs presented to two verifiers are engineered to be uncorrelatable. Optional, consented same-human binding lets two issuers confirm one living person without exchanging biometric data.

VERIFIABLE CREDENTIALS

Where it applies

- KYC and reusable KYC
- Age and eligibility proofs
- Selective-disclosure credentials
- Healthcare, voting and e-prescriptions



SENSECRYPT KYA: KNOW YOUR AGENT EARLY ACCESS

Give AI agents authority tied to a verified human.

Each agent receives a verifiable credential authorized by a biometrically verified human, recording who authorized it, its scope and its expiry. A person can approve privileged actions by face.

The chain

01 **Human VC:** a biometric verifiable credential establishes the accountable human.

02 **Agent VC:** the human signs the agent's credential, embedding model hash, scope and expiry.

03 **Agent key:** a per-action key pair with a transient private key.

04 **Per-action signature:** connected tool calls are signed, reducing reliance on API keys and bearer tokens.

Five questions, every action

WHO	Traced to a verified human by a cryptographic chain.
WHAT	Model hash and scope in the agent certificate.
WHEN	Credentials that expire in minutes, not months.
WHY	Signed intent: the instruction that started it.
HOW	An authenticated tunnel, no public tool exposure.

Connected applications must enforce the permissions the credential records.



WHERE IT FITS

One root of trust. Every sector that needs one.

Wherever a decision depends on knowing the real person, SenseCrypt puts a live face behind it.

Government

National eID without a biometric honeypot, verified offline at the border and in the field.

Financial services

Re-verify the person and bind high-value actions to a living person, keeping no template database.

Payments

Approve the payment with a live-face check on the customer's own phone.

Enterprise

Kill the password, keep your IAM: passwordless workforce sign-in that coexists with your estate.

Healthcare

Access that follows the clinician from station to station on the ward.

Manufacturing

Shift change in seconds on shared terminals, not shared logins.

Retail

Smoother checkout for shoppers, faster starts for crew on the floor.

Logistics

One identity for every depot, driver and partner across the network.



INTELLECTUAL PROPERTY

Our inventions. Patented.

The ideas behind SenseCrypt are protected by patents. Here is what they cover, in plain words.

Method and system for implementing a privacy-preserving, face-based protected public key infrastructure

Digital certificates that only your face can unlock.

- Your face generates the public key and a privacy-preserving, disposable face token when you register. The matching private key can only be regenerated from a fresh capture of the same face.
- The user's identifier is held only in encrypted form, so the server never holds your face or readable personal details.
- Context-bound certificates: each certificate is tied to one context, such as one bank or one login, so it cannot be reused anywhere else.

Why it matters: PKI, the trust system behind secure websites and digital signatures, now anchored to a live person. It powers SenseCrypt PKI and eID.

Systems and methods for decentralized recoverable storage of private data and anonymized, confidential message exchange secured by user biometrics

Recover your data with your face.

- Your face and a PIN create temporary keys on your own device. They lock a recovery token and are then thrown away, never stored.
- Your private data sits in an encrypted store that the backup service keeps but cannot open.
- Recovery needs no central password store, email reset or SMS code, the routes used in SIM-swap and social-engineering takeovers. The same approach protects confidential, anonymized messaging.

Why it matters: account recovery is where most security breaks. This patent makes the live person the recovery key.

Additional patent applications are pending.

EVIDENCE YOU CAN CHECK

We publish the evidence.

Each claim travels with its boundary attached, so your procurement and security teams can check it.

NIST **Evaluated in NIST FRTE since 2021**

Under Seventh Sense's own name, most recently 1:1 (July 2024) and 1:N (September 2024). This is recognition-algorithm evaluation, not certification.

PAD **iBeta Level 1 & Level 2 liveness**

Presentation-attack testing to ISO/IEC 30107-3, within the tested component and attack conditions. Injection attacks are handled by separate controls: app attestation and device checks on phones, secure terminals for webcam.

IP **Multiple patents**

Including face-based PKI and biometric-secured data recovery. See page 13.

DEV **Public documentation**

Python, Android and iOS SDKs plus a REST API, documented at sensecrypt.com/idp-docs and sensecrypt.com/eid-docs.

STD **Standards you already run**

FIDO2 / WebAuthn, OIDC, OAuth 2.0, SAML 2.0, SCIM 2.0 and FAPI 2.0.

In the field

NUS Singtel HP Finexus Intercorp Unico LatinID ST Engineering

GET STARTED

Bring your hardest identity problem.

A credential that must verify with no network. A signature others can verify. A fleet of AI agents that must answer to named humans. Tell us the problem, and we'll show you the mechanism, not a slogan.

Works with what you run.

Deployed alongside your existing IAM, hosted or on-premises.

Enterprises & governments

Discuss a deployment

seventhsense.ai/contact

Developers

Read the documentation

sensecrypt.com/idp-docs
sensecrypt.com/eid-docs

Try SenseCrypt IdP

Start a 30-day trial

sensecrypt.com

Design partners

ZKP and KYA early access

contact@seventhsense.ai

SEVENTH SENSE

The face of a smarter, safer future.

SenseCrypt ties identity, access, signatures and AI-agent authority to a live person, with zero biometric storage and private keys that never exist at rest.

101 Cecil Street #11-01, Singapore 069533

seventhsense.ai · sales@seventhsense.ai

Product availability as of October 2026. Specifications are subject to change.
SenseCrypt is a trademark of Seventh Sense Artificial Intelligence Private Limited.