



SILENT KEY TECHNOLOGIES, RIYADH

Silent Key

Built on silence.

بني على الصمت

Privacy is engineered, not promised. Your data does its work and leaves no trace, and nobody, ourselves included, ever holds a key that can read it.

Privacy

Cybersecurity

AI

Two patents filed at SAIP

INVESTOR DECK 2026

PRE-SEED ROUND OPEN

Silent Key Technologies, Riyadh NOAI+ SilentSpace SilentBOX BurnKey Kontra+

THE PROBLEM

Every answer today asks you to trust someone who holds your key.

01 AI

Data leaves to be useful

Staff paste names, ID numbers and diagnoses into AI models run outside the Kingdom. Afterwards nobody can show what left, or to whom.

02 SOVEREIGNTY

It has to stay here

Banks answer to SAMA's Cyber Security Framework, and data localisation now sits with the National Data Management Office at SDAIA. A foreign platform cannot meet that by promise.

03 KEYS

Or it is lost with you

Crypto and private records reach an heir only if someone else holds the keys or the custody. And deleting data is a promise, never a proof.

OUR ANSWER

A machine that decides the fate of a key it never holds.

1 Hide

NOAI+ lets AI do the work on placeholders, then puts the real values back. The model never receives the names.

2 Keep

SilentSpace runs the whole application stack on the customer's own servers, inside the Kingdom.

3 Release

Conditional release opens a vault to the right person only when the owner's conditions are met. Crypto inheritance without handing over keys.

4 Destroy

BurnKey erases on command and issues a receipt anyone can verify offline.

We hold nothing. Data stays with its owner, only the minimum ever leaves, and every action leaves signed proof. Content is encrypted on the owner's device with published standard cryptography; a breach of our servers yields only ciphertext. We can be compelled to deny service. We cannot be compelled to read data.

INTELLECTUAL PROPERTY

Two Saudi patent applications on the mechanism, not on an app.

WORLD-STATE DISPOSITION | SA 1020267700

Filed 20 August 2026

An autonomous evaluator decides the fate of a key it never holds, with delivery and erasure as its two outcomes. One filing covers both the inheritance handover and verified destruction.

DISTORTION SHIELD | SA 1020266962

Filed 10 August 2026

Routes what an encrypted vault shows by the outcome of authentication, so an unlock forced under duress opens decoy content and the real vault stays sealed.

Why mechanism level. A claim on a vault protects one app. A claim on the mechanism follows it into wallets, custodians, password managers, estate technology and escrow. SilentBOX and BurnKey are the first two things we pointed it at. Both applications are filed at SAIP and not yet granted; full specifications are shared under NDA.

BUILT AND RUNNING

Six products, one principle. Four in people's hands.

PRODUCT	WHAT IT DOES	STATUS
NOAI+	Privacy gateway that lets a company use AI without sending personal data, in Arabic and English	Live gateway since 7 Oct 2026
SilentBOX	Encrypted vault app; the passphrase never leaves the phone	Live on Google Play
BurnKey	Destroys data on command and issues a receipt verifiable offline	Live on Google Play
Kontra+	Contract risk review for Gulf construction	Live in Riyadh on SCCC, stc's Saudi cloud
SilentSpace	The application platform that never leaves the Kingdom, on the customer's own servers	Running demo, in build
Release engine	Conditional release by API for wallets, custodians and estate technology	Design stage

LEAD PRODUCT | NOAI+

It delivers what it cannot see.

WHAT THE NURSE TYPED

Draft a reminder for our patient **Fatima Al-Harbi**, ID **1098765432**, phone **+966 55 123 4567**. She has **type 2 diabetes** and starts **insulin** next week.

WHAT THE AI MODEL RECEIVED

Draft a reminder for our patient **[PERSON_1]**, ID **[ID_1]**, phone **[PHONE_1]**. She has **[MEDICAL_1]** and starts **[MEDICAL_2]** next week.

The AI writes the answer. NOAI hides the names before they leave your machine and puts them back when the answer returns, with a signed receipt of exactly what was sent. Live test, 13 Oct 2026, 40 made-up Saudi patient files and contracts: **0 of 440** planted private values reached the model, **160 of 160** restored exactly, **428** automated tests passing. Open source under Apache 2.0.

SOVEREIGN PLATFORM | SILENTSPACE

Residency proven by the customer's own kernel, not promised by us.

6 in 1

The whole stack

Database, API, logins, file storage, live updates and server code, on the customer's own hardware, run from one screen in Arabic or English.

0 of 48

Peers outside

On a reference install, ten components and forty eight network peers, none outside the local network. The customer runs the count.

12 of 21

Controls met

In our published control mapping, with seven partial and two gaps named openly. The serious gap is encryption at rest.

Small

Not a rack

773 MB idle on a 6.7 GB baseline. A small server is enough to run it.

[Stated plainly.](#) The mapping is our own assessment, not an accreditation. For banks the binding text is SAMA's Cyber Security Framework, section 3.4.3; data localisation now sits with the National Data Management Office at SDAIA.

WHERE THE PATENT GOES

Six industries, one problem: no spare key allowed.

01

Crypto inheritance

Releases to an heir without giving anyone the keys or an exchange custody.

WALLETS, EXCHANGES, CUSTODIANS

02

Proof of destruction

The PDPL obliges erasure on request. A receipt a regulator can verify replaces a written assurance.

CLOUD VENDORS, PROCESSORS

03

Dormancy and estates

A quorum of a law firm and a family member, with a veto window, makes handover procedural.

PRIVATE BANKS, TRUSTEES

04

Escrow without an agent

The mechanism is the intermediary, and it cannot read what it holds.

LAW FIRMS, NOTARIES

05

Break glass access

Emergency access with no recovery key sitting on a vendor's balance sheet.

PASSWORD AND IDENTITY VENDORS

06

Release on a verified event

Insurance files, medical directives and embargoed records: open only when something is true.

INSURERS, HEALTH SYSTEMS

Stated as direction, not pipeline: the release engine is at design stage and no licensee is signed.

BUSINESS MODEL

Priced today. Licensed tomorrow.

SILENTSPACE

SAR 113,000

first deployment

Licence SAR 18,000, deployment and hardening SAR 55,000, compliance evidence pack SAR 40,000. Then SAR 35,000 a year.

NOAI+

USD 300

a month per company

KONTRA+

SAR 2,400

per contract review

LICENSING THE ENGINE

An API priced per vault or per seat, so a wallet or password manager ships conditional release without building it.

White label inside partners, or licence the patent itself. Highest margin, and why the claims were drafted at mechanism level.

TEAM AND ASK

Built, filed and running. Now the first signature.



Ramzi Hobeishy

Founder, Riyadh. Designs and ships every Silent Key product and both patent filings. Full time on Silent Key from November 2026.

WHAT THE ROUND COMPLETES

- The Saudi entity, so a regulated buyer can contract and be invoiced
- An independent security audit, which turns architecture into evidence
- PCT filing for both applications inside the twelve month window

rhobeishy@gmail.com silentkeytechnologies.com

- 1 A first regulated pilot**
A bank, hospital or government supplier running SilentSpace or NOAI+ on its own servers.
- 2 Introductions**
Security, data protection and digital asset leads in the Kingdom.
- 3 USD 500,000 to 1,000,000 pre-seed**
For the entity, the audit, the first paid pilot and the first hires.