

AUTHENTICATION FOR THE AI ERA

One unclonable hardware token. Already in every customer's hand.

Every smartphone camera sensor carries a **factory-random, non-copyable silicon fingerprint**. ToothPic turns it into a hardware security key: nothing to ship, nothing to store, issued in a single app update.

7B+

devices already carry the token

€0

marginal cost per authentication

30 ms

invisible to the user*

Where it's used and what it delivers

For banks, payment providers, insurers and fintechs



Login & app access

Replaces passwords and SMS OTP with an unclonable hardware key.

99.99% account-takeover risk removed


Payment & transaction signing

Invisible, PSD2/3-compliant SCA for transfers and instant payments.

€9–20M SMS OTP spend saved per 10M users


Device binding & re-enrolment

New phone, reinstall or reset without SMS, helpdesk or branch visit.

up to 50% less device-ID maintenance


Fraud back-office efficiency

A deterministic signal auto-clears false alerts and unmaskers emulators and mule farms.

70% analyst time reclaimed


Contact-centre verification

A push to the customer's own phone verifies the caller and shortens call handling.

1 tap replaces security questions


Deepfake-proof video & voice

Remote onboarding, KYC and executive approvals: a real phone must sign.

€95M wired out of an Italian bank after an AI voice-clone scam (2026)

The problem: AI now fakes identity at scale

- Anything **known** can be phished
- Anything **shown** can be faked
- Any **person** can be synthesised
- Any **camera feed** can be injected

OTPs, passwords, face and voice checks are all software signals — and GenAI manufactures software. **Only physical possession still settles who is really there.**

How it works: the token is the camera sensor


Read Sensor noise pattern (PRNU) via the standard camera permission.

Rebuild A standard elliptic-curve key is regenerated in ~30 ms to sign the challenge.

Vanish Key destroyed after signing. Nothing on the phone, nothing in a database.

0 SECRETS AT REST

DEFEATS INJECTION ATTACKS

FIDO2 · U2F

Hardware-token security with software-token economics

	UNCLONABLE & HW-BOUND	SURVIVES RESET	VENDOR INDEPENDENT	USER FRICTION	COST
SMS OTP / SIM binding Transferable by design	×	✓	×	Read & type	€€
Passkeys Synced by design	×	✓	~	Prompt	€
Secure enclave Erased on reset	~	×	×	Biometric / PIN	€
Hardware token Dedicated physical key	✓	✓	✓	Carry & press	€€€
ToothPic Bound to camera silicon	✓	✓	✓	Invisible	€

Runs beside your stack — not instead of it



- Zero database changes** — only standard public keys
- 100% on-device** — no biometrics or keys leave the phone; GDPR-clean
- Weeks, not quarters** — a plugin next to your current SCA

Validated. Certified. In production.

4 paid EU deployments

Insurance, payments & academia, live in production

400M+ users

Proof of concept on a real-time payments platform

4 patent families

US · EU · CN · JP · IL · KR, 20-year terms

FIDO2 + U2F

Certified. Politecnico di Torino spinoff, 2 EIC Seals of Excellence

90 days to proof. One flow. Your own data.

WEEKS 1–2 Scope

Pick one journey, freeze the baseline

WEEKS 3–10 Pilot

SDK runs silently beside your SCA

WEEKS 11–13 Decide

Fraud lift, false rejects, latency, NPS


EMAIL
info@toothpic.eu

WEB
www.toothpic.eu

Existing controls stay live. Reversing costs one sprint. **Let's talk.**