TOOTHPIC CALLER VERIFICATION

Is it really your CEO on the call? Prove it in one tap.

Generative AI now clones a person's **voice and face in real time**, so passwords, OTPs and biometrics can be faked or intercepted. ToothPic Caller Verification moves trust to the **physical camera sensor** of the caller's smartphone: a deepfake has no sensor, so it cannot answer the challenge.

The problem: anyone can sound like your CEO

- Voices are **cloned** from seconds of audio
- Faces are **simulated** live on video
- Credentials are **phished** or intercepted
- Keys in the OS are **stolen** by malware

€95M

wired out of an Italian bank in 2026 after an **AI voice-clone and fake-executive scam**. One verified call would have stopped it.

How it works: out-of-band, hardware-signed



Challenge During the call, the verifier sends a one-time challenge by secure push.

Sign The other phone reads its camera-sensor fingerprint (PRNU) and rebuilds a private key to sign.

Verify & vanish The signature is checked against the stored public key; the private key is destroyed.

DEFEATS VOICE & VIDEO DEEPFAKES

COURT-ADMISSIBLE PROOF

Where it's used

For banks, insurers, payment providers and any executive team

Executive impersonation protection

Stops voice clones and video deepfakes of executives during live transactions and approvals. Also secures remote hiring against synthetic candidates.

Secure out-of-band channel

A second channel anchored in the camera sensor, giving tamper-proof, court-admissible proof of who was on the call.

IAM outage business continuity

Keys are bound to hardware sensors, not databases, so verification keeps working when core IAM systems are offline.

Emergency backup for compromised IT

A clean verification path even if corporate IT, network or directories are fully compromised.

FOR THE CIO & CISO · INTERNAL THREATS

Protect your people from social engineering

Employees are probed and targeted with deepfakes. ToothPic adds a **decentralised, out-of-band channel** bound to each phone's sensor, so software credentials alone can never pass as a colleague.

FOR THE CCO & CMO · EXTERNAL BRAND TRUST

Stop fake executives reaching your clients

Attackers impersonate executives on calls to push fraudulent transactions. **Caller 1 instantly verifies Caller 2 is genuine**, neutralising impersonation before money moves.

See it live. One tap, one verified caller.

STEP 1
Demo
Watch a live caller verification end to end

STEP 2
Pilot
Roll out to an executive or treasury team

STEP 3
Scale
Extend to contact centre and partners

Runs beside your existing IAM. **Let's talk.**

EMAIL
info@toothpic.eu

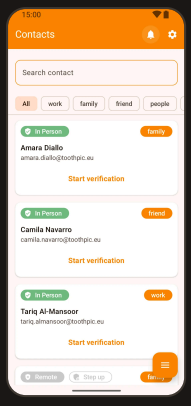
WEB
www.toothpic.eu

Continued overleaf: the verification flow, step by step.

LIVE CALL VERIFICATION

Six steps. One tap. No secrets stored.

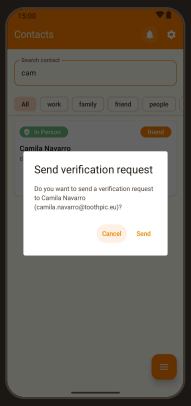
Robert (the verifier, on Android) wants to be sure that Camila (on iPhone) is really on the call. Here is what each of them sees.



STEP 01 · VERIFIER

Search directory

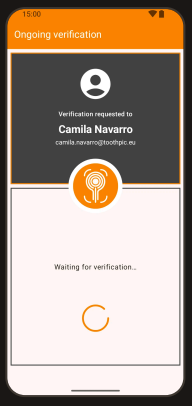
Robert opens Caller Verification during the call and finds Camila.



STEP 02 · VERIFIER

Send challenge

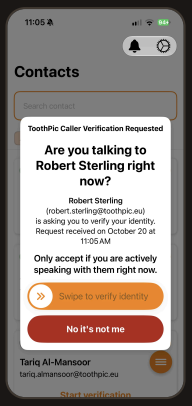
A one-time challenge is created locally and sent out-of-band.



STEP 03 · VERIFIER

Waiting

The push is delivered; Robert waits for the signature.



STEP 04 · VERIFIED

Confirm request

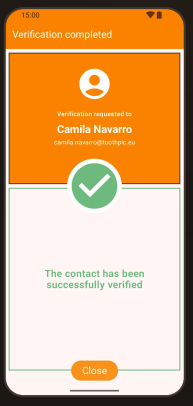
Camila gets an alert on his own iPhone and swipes to confirm.



STEP 05 · VERIFIED

Photon capture

The SDK estimates the sensor fingerprint, rebuilds the key without exposing it in RAM, signs and purges it.



STEP 06 · VERIFIER

Verified ✓

Robert's app checks the signature against Camila's public key.

Authentication complete ✓ Ephemeral private key purged from memory. Hardware identity verified.

Under the hood: the hardware-anchored flow

00 — User directory
The backend pre-stores every registered user's public key.

01 — Initiate
Caller 1 selects Caller 2 and sends a challenge by secure push.

02 — Hardware sign
Caller 2 signs with a key generated only by their phone's physical camera.

03 — Verify
Caller 1 validates the signature with the stored public key.

04 — Notify
Instant result: verified, or failed (AI, wrong device, timeout).

Why software-only security fails in the AI era

AI attacks the top of the stack. Generative models now defeat biometrics, software tokens and OTPs, and injection attacks bypass the camera feed entirely.

Storage is not trust. Keys kept in the OS or firmware can still be stolen by system-level malware.

The ephemeral ideal. ToothPic never stores a credential. The key is rebuilt from the sensor only when needed and destroyed straight after. Steal the storage and you still have nothing without the physical sensor.

- **7 · AI / GenAI layer** — VULNERABLE: BIOMETRICS, TOKENS, OTP
- 6 · Application
- 5 · Middleware
- 4 · OS
- 3 · Driver
- 2 · Firmware
- **1 · Hardware (camera sensor)** — TOOTHPIC TRUST: PRNU ANCHOR

Make every high-value call provably genuine.

Part of the ToothPic platform: the same sensor key also secures login, payment signing, device binding and fraud operations.

EMAIL
info@toothpic.eu

WEB
www.toothpic.eu

Ref.: aligned with Gartner, Areas of Focus for Addressing Disinformation Attacks; Emerging Market Quadrant for Deepfake Detection Startups (Jul 2026).