

A verified number isn't a verified identity.

OTP confirms a number can receive a code. It never confirms the SIM is still in your customer's phone, or that this is the same SIM and device you onboarded. Sign3 SIM Binding closes that gap, silently, on every sensitive action.



No OTP

Nothing to phish, forward or intercept



Every action

Re-checked silently on sensitive events



SIM, eSIM, iSIM

Cryptographic check over mobile data

WHY OTP ISN'T ENOUGH

The number can stay the same while the SIM changes.

A SIM swap can redirect OTPs to another device. Code delivery alone doesn't prove the setup you trusted.

See beyond code delivery

Adds context about the mobile subscription and its relationship to the device or app.

Spot relevant changes

Surface inconsistencies in the expected SIM and device relationship for risk assessment.

Make informed decisions

Use the signal in your existing controls for step-up, review, hold or block.

HOW IT WORKS

From mobile signals to the right action



01 — BIND

Establish the expected setup

At onboarding, link the mobile subscription, device and app environment.



02 — CHECK

Assess sensitive activity

Evaluate signals at login, device registration or any sensitive action.



03 — FLAG

Surface a change

Identify a SIM or device mismatch that warrants closer scrutiny.



04 — ACT

Apply your risk rules

Feed the signal into your fraud flow for step-up, hold, review or block.

THE SILENT BIND, STEP BY STEP

No OTP. No code to phish, forward or intercept.

The SIM proves itself to the network, and the network returns the result.

01

Initiation

The customer enters their mobile number in your app.

02

Cellular routing

Runs over mobile data, not Wi-Fi. The number must be live on the network.

03

Cryptographic handshake

The network challenges the SIM (RAND). Both sign a response (SRES) with a key (Ki) that never leaves either side.

04

Silent verification

The network confirms the active SIM maps to the registered number (MSISDN).

05

Bind token

You receive a signed bind token. The customer never sees or types a code.

WHERE IT ADDS VALUE

Mobile identity context for critical journeys



Account access and takeover

Add a mobile identity signal to login and sensitive account actions.



Digital lending

Assess SIM and device patterns at onboarding and during account activity.



High-value payments

Use relevant changes as an input to risk-based transaction checks.



Device registration

Establish an expected mobile setup early, where supported.

STRONGER IN COMBINATION

Four signals, read together, are hard to beat

01

Mobile identity

The SIM, its carrier and its relationship to the device.

02

Device intelligence

A persistent device identity that survives resets and reinstalls.

03

Authentication

The result of the verification step the customer just completed.

04

Behaviour and transaction

Whether this action fits how this account normally behaves.

A fuller picture of mobile identity risk, without treating every SIM change as fraud.

The customer taps once. The SIM does the proving.

Trusted by 20+ banks, NBFCs, and fintechs across India

[Book a demo](#) →

sales@sign3labs.com · sign3.ai