UNIBEAM

ONLY ONE IS SIM-NATIVE:

Redefining Business Transaction Authentication with Unibeam

A Unibeam White Paper
May 2025

Contents

Executive Summary

→ Business transactions are at high risk for fraud

Transferring money, making a one-click purchase, or logging into a marketplace – all these require strong, real-time user authentication.

→ “SIM-based” often means “network-based”

Most solutions rely on mobile operator records and databases - not the SIM itself - making them vulnerable.

→ Network trust breaks down at the transaction level

Legacy protocols, static identifiers, and human error all extend the attack surface and weaken the security of mobile networks when real money or sensitive data is at stake.

→ Unibeam authenticates from inside the SIM

Unlike other solutions, Unibeam verifies authentication identifiers directly from the secure SIM chip – the only solution providing such deterministic authentication.

→ Real-time SIM swap protection

Unibeam instantly detects SIM and device changes and blocks fraudulent transaction attempts before they succeed.

→ No apps, SDKs, or device customization needed

Unibeam works silently or interactively across all SIM and eSIM-enabled devices, without code changes, software installs or OS permission updates.

→ The only truly SIM-native solution

Others rely on the network. Unibeam starts inside the device - where real trust begins.

The Business Transaction Challenge

User authentication plays a critical role in business transactions - like transferring money, making a one-click purchase, or signing in to shop on a marketplace. These actions may seem routine, but they carry real risk. If the wrong person gets through, the result can be fraud, lost revenue, or stolen data.

Other solutions claim to offer “SIM-based” authentication, but most don’t actually use the SIM card itself. Instead, they pull SIM-related data from mobile network databases. This expands the attack surface - exposing the entire mobile network and its databases to potential attacks. That’s not secure enough when sensitive data, financial transactions, or real-time authentication are involved.

To properly secure these kinds of actions, authentication needs to come from a more trusted source - one that attackers can’t spoof or intercept. The SIM chip, with its built-in secure enclave, offers exactly that.

This paper explains why business transactions need a stronger foundation for authentication, and why only Unibeam delivers it - by verifying the user directly from inside the SIM, not the network.

The Myth of Network-Based SIM Authentication

Many authentication providers claim to offer SIM-based security - but in reality, most rely on the mobile network, not the SIM itself.

Here's how it works: when a user tries to log in or complete a transaction, the provider's application asks the mobile operator for basic SIM-related information – the phone's IP address, the phone number (MSISDN), device ID (IMEI), or SIM ID (ICCID). The operator's system checks its records and confirms whether the data matches. This process is called "silent authentication" because it happens in the background, without the user's input.
That might be enough for low-risk logins. But for transactions involving money or sensitive data, it's a critical gap. The reason? These systems never actually talk to the SIM card - they talk to the network's version of the SIM. That version can be out of date, spoofed, or even manipulated by an attacker. And because the mobile operator is part of the process, its infrastructure becomes part of the risk.

What's more, silent authentication cannot detect SIM swaps - the leading form of SIM-based fraud. To address this, businesses need to add a separate SIM swap check via API, which increases latency and cost - and still relies on network data instead of the SIM.

Network-based SIM authentication is easier to deploy due to its centralized database structure - but it relies on the assumption that the network is accurate and secure. That assumption no longer holds.

To eliminate these weaknesses, authentication must move inside the SIM itself - where the data is secure, current, and untouchable by external actors. Only then is it truly SIM-based.

Four Reasons Networks Aren't as Secure as the Secure SIM Enclave

Even though many systems still rely on them as the gatekeepers of identity, legacy mobile network protocols and architecture were never designed to handle secure online authentication. Why?

Outdated signaling makes interception easy

Mobile networks still rely on outdated signaling protocols like SS7, which lack proper encryption and are susceptible to interception or manipulation. This makes it possible for attackers to hijack one-time passwords, intercept login tokens, or redirect transaction approvals.

Silent authentication solutions often depend on detecting a user's mobile data IP address - which only works when the phone is off Wi-Fi. Since most devices are connected to Wi-Fi by default, these solutions require additional SDKs, scripts, or code changes to function. These workarounds not only add complexity but also expand the attack surface.

Operators are a single point of failure

Network-based authentication depends on mobile operator systems and employees. Insider threats, misconfigurations, or social engineering can all lead to compromised user data - even without malware or device access. If an attacker exploits this weak point, they can gain access to user accounts and authorize high-value actions like money transfers or purchases.

Static identifiers are easy to exploit

Network-based methods rely on fixed identifiers like the IMEI and MSISDN, which can't be rotated or customized per session. This means that once they're exposed, it's easy for attackers to

reuse these identifiers. Since the IMEI is tied to the device and the MSISDN to the SIM, both become persistent risks for fraud in business transactions.

SIM swap fraud still bypasses the network

Networks can't stop SIM swap fraud. Attackers can convince operators to transfer a user's number to a new SIM, effectively taking over their identity. Network-based systems often can't detect the change fast enough. And once a number is transferred, attackers can intercept transaction codes or reset credentials to complete unauthorized purchases or bank transfers.

The fact is that authentication that depends on the network inherits all of its weaknesses. True security requires a model that's independent of the mobile network - and that starts with the SIM itself.

Unibeam's SIM-Native Breakthrough

For any action where money or sensitive data is at stake, authentication must be tamper-proof and real-time – and that starts with the SIM. That's why Unibeam places the authentication process inside the SIM card's secure enclave - the same type of tamper-resistant chip used in bank cards.

Instead of relying on the mobile network to verify device identity, Unibeam operates directly within the SIM hardware. This means the identifiers used for authentication are created and managed securely inside the SIM itself - not by the mobile operator.

With Unibeam, every SIM becomes a trusted and up-to-date cryptographic device. It can generate its own secure, enterprise-specific identifiers and transmit them over fully encrypted channels - with no involvement from the mobile network. No app, no SDK, and no access to fragile network infrastructure required.

This makes Unibeam the only solution that delivers true SIM-native authentication. It bypasses the vulnerabilities of network-based methods and gives enterprises direct, hardware-level control over mobile identity.

Even better, Unibeam works on all SIM and eSIM-enabled phones globally, including feature phones and smartphones, without requiring any device modifications.

With Unibeam, enterprises gain full control over mobile authentication. Instead of trusting a mobile operator's pass/fail response, Unibeam delivers deterministic hardware-level identifiers and user responses directly from the SIM's secure enclave. This enables a true zero-trust model: the enterprise makes its own authentication decisions based on trusted data - not third-party assessments.

What Makes SIM-Native Better

Feature	Network-Based Solutions	Unibeam (SIM-Native)
Authentication Origin	Network operator infrastructure	Inside SIM secure enclave
Identifier Type	Static (IMEI, MSISDN)	Dynamic per-user, per-enterprise
Encryption	Dependent on MNO	AES256 from SIM to endpoint
SIM Swap Detection	Indirect or delayed	Built-in, immediate
Deployment	SDKs, scripts, device-specific code	Works across all SIM/eSIM devices
Consent Capability	Silent only	Supports active user approvals

Security and Flexibility, Built In

Unibeam is built to meet the two things every business transaction needs: strong security and a smooth user experience. Whether it's logging into a bank, confirming a payment, or making a one-click purchase, Unibeam authenticates the user directly from the SIM - no apps, no SDKs, and no special code required.

It supports both silent and interactive modes. That means it can quietly verify a login or session in the background, or prompt the user to approve a transaction - without disrupting the flow. And because it runs entirely inside the SIM's secure chip, every step is protected at the hardware level.

One of Unibeam's biggest advantages is how it handles SIM swap attacks - where hackers trick mobile carriers into moving a number to a new SIM, then take over calls, texts, and accounts. Most systems can't catch this in time. Unibeam can. It monitors the SIM from the inside and immediately blocks anything that looks suspicious - before any damage is done.

Even if a phone is lost or stolen, an attacker still can't get past Unibeam. The cryptographic data inside the SIM can't be copied, spoofed, or extracted.

People can be tricked. Networks can be fooled. But the chip can't - and that's what makes Unibeam ideal for real-world transactions that can't afford to go wrong.

UNIBEAM

About Unibeam

At Unibeam, we're redefining user authentication for service providers and enterprises by seamlessly authenticating customers through SIM/eSIM and mobile device data. No passwords, no intrusive questions – just a secure, frictionless user experience.

For more information, please visit www.unibeam.com