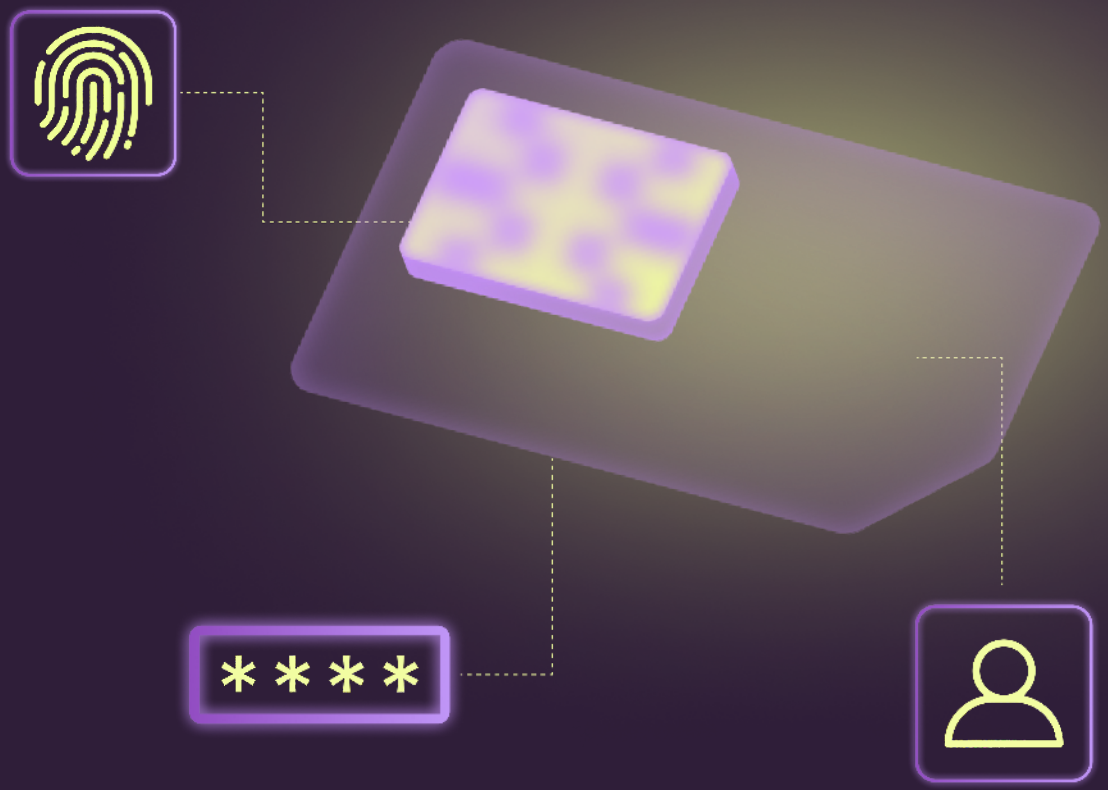
UNIBEAM

Deterministic by Design:
The Case for SIM-Based Authentication

A Unibeam White Paper
April 2025



Contents

Executive Summary 3
Explainer: Probabilistic Vs. Deterministic 4
The Limits of Probabilistic Authentication.....5
AI Makes Probabilistic Authentication Weaker.....6
The Problem with Biometrics.....7
Why SIM-Based Authentication Works 8
Combining SIM Authentication with Biometrics.....9
A Simpler Path to Privacy and Compliance.....11
The Bottom Line 12
About Unibeam.....13

Executive Summary

→Probabilistic authentication falls short

Most authentication systems today rely on risk scores based on user risk signals. These systems estimate rather than verify identity — and estimations can be wrong.

→False outcomes create real problems

Probabilistic methods often block legitimate users and let fraudsters through. These errors lead to lost revenue, poor user experiences, and security gaps.

→Heavy data collection adds cost and risk

To function, probabilistic systems require extensive user tracking. This increases compliance burdens, privacy concerns, operational complexity, and, consequently, the overall cost.

→AI is making it worse

Attackers now use AI to mimic legitimate behavior and bypass risk-scoring systems. Fraud AI tools are unrestrained by privacy and regulations and are evolving faster than defenders can respond.

→Biometrics aren't deterministic

Biometric and syncable passkeys confirm access to a device, not identity. They can be shared, synced across devices, or bypassed with PINs.

→SIM-based authentication is deterministic

A SIM card provides a fixed, tamper-proof ID issued by a secure element inside the SIM. The result is a clear, binary deterministic match — no scoring, no guesswork.

→Harder to fake, easier to trust

The SIM ID is stored in a hardware secure element that attackers can't reach. It can't be cloned, copied, or altered by malware or AI.

→No personal tracking required

SIM-based authentication works without collecting behavioral data. This reduces privacy risk and simplifies compliance.

→Stronger with biometrics

When combined with on-device biometrics, SIM authentication offers strong, layered security without weakening user experience.

→Built for today's threats

SIM-based authentication delivers precision, privacy, and resistance to manipulation — and it's built to meet the demands of modern identity.

Explainer: Probabilistic Vs. Deterministic

→ Probabilistic means something is based on probability - a best guess using several available data-points and information.

→ Deterministic means the outcome is certain - the same input always gives the same result.

In authentication, probabilistic systems don't confirm identity directly. They look at signals like device type, IP address, and behavior patterns. Then they calculate a risk score that reflects how likely it is that the user is legitimate. The system uses that score to decide whether to confirm identity and allow or block access.

Deterministic systems do the opposite. They check something fixed and secure - like a SIM card's ID - and match it to what's expected. There's no scoring or guesswork. The system either confirms the match or it doesn't.

Probabilistic is about likelihood. Deterministic is about proof.

The Limits of Probabilistic Authentication

Many authentication systems today are probabilistic. They rely on risk scores based on signals like device type, location, and user behavior. These systems estimate whether someone is a real user or a threat — but they can't say for sure.

And of course, estimates can be wrong. Real users are frequently blocked, while fraudsters slip through. These errors frustrate security teams, turn away paying customers, and leave systems open to attack.

What's more, to generate risk scores, probabilistic systems require constant access to personal data. Every login or transaction must be tracked, analyzed, and evaluated in real time. This includes IP addresses, devices, browsing habits, location, call information, and behavioral patterns — all of which are considered sensitive under laws like GDPR and CCPA.

That adds legal risk, operational complexity, and growing compliance costs. It also creates trust issues. Users don't like being tracked, and constant monitoring can damage brand reputation and user experience.

The more data a system needs to guess who someone is, the more it increases exposure — not just to privacy concerns, but to attacks as well. In an environment where signals can be faked, copied, or manipulated, probabilistic authentication leaves too much room for error.

AI Makes Probabilistic Authentication Weaker

Fraudsters now use AI to beat the same systems designed to stop them — especially probabilistic authentication. These systems rely on patterns and risk signals to decide whether a user is real. AI can study those patterns, copy them, and fool the system into thinking that a fake user is legitimate.

The more data attackers gather, the more realistic their attempts become. They can test and refine their approach until they find a way through. In many cases, their tools are just as advanced as the AI built to stop them.
While protection AI tools are governed and restrained by privacy and regulatory constraints, the AI tools used by fraudsters do not have any self-imposed limits. Ask ChatGPT how to hack into a user web account and ChatGPT will answer it cannot help with that. Ask the same question to one of the many dark web LLMs and you will get a step-by-step explanation on how to go about it.

If you need to impersonate someone, ask ChatGPT for the personal address and birthday of an individual and you will not get an answer. Ask the same question to a fraud oriented LLM and you will get a bot crawling for personal and private information of anyone.

Attackers also move faster. They don’t worry about ethics, rules, or privacy laws — they just focus on results. This leaves defenders scrambling to adjust scores, retrain models, and patch new loopholes. It becomes a constant race with no finish line.

Probabilistic systems weren’t built for this kind of threat. Against AI-powered fraud, they’re too slow, too reactive, and too easy to outsmart.

The Problem with Biometrics

Biometrics are often seen as a secure way to verify identity, but they are not always the most reliable option. Most systems use biometric passkeys to make the user experience easier — but this does not guarantee that only one same person and identity can access an account.

The reason is that passkeys can sometimes be tied to the device, not the individual. If more than one fingerprint is registered on the same phone or tablet, any of those users can pass the biometric check. This is especially true with fingerprint sensors, which often support fingerprints of multiple users. A person may register their own fingerprints but the fingerprints of one of their kids, to let them play videogames.

What's more, some systems allow passkeys to sync across devices with the same account. A passkey created on an iPhone, for example, can be copied to an iPad. The iPhone may unlock with the user's Face ID, while the same passkey could be accessed and unlocked on the iPad using a child's fingerprint. The system accepts both as valid.

Most devices also include a PIN fallback. If someone guesses or tricks a user into sharing their PIN, they can unlock the passkey without needing a biometric match at all.

Biometrics are convenient to use to enter or re-enter credentials on a trusted device, but they don't offer certainty. They confirm access to a device — not identity. Without a fixed, tamper-proof signal like a possession SIM-based ID factor, and knowledge MFA,biometric inherence alone can leave a critical gap in authentication.

Why SIM-Based Authentication Works

SIM-based authentication doesn't rely on signals or scores. It confirms identity using a unique identifier stored on the SIM card — one that is fixed, issued by a secure element in the SIM card and can't be faked or changed.

This makes SIM-based authentication deterministic. The system doesn't analyze behavior, assign a risk level, or guess. It either sees the expected SIM ID or it doesn't. The result is a clear, binary decision — without gray areas.

The SIM ID is stored in a secure part of the chip that malware, apps, and browsers can't access. It stays protected at the hardware level and is shielded from manipulation by attackers, AI tools, or social engineering. It can't be cloned, guessed, or impersonated.

Unlike probabilistic systems, SIM-based authentication doesn't require collecting hundreds of data points. It doesn't track users, build profiles, or scan behavior. This reduces privacy risk, lowers compliance overhead, and simplifies the entire authentication flow.

A deterministic match from a SIM ID tells the system exactly who is connecting — without relying on unpredictable or easily faked inputs. It delivers a level of certainty and resistance that probabilistic and biometric methods can't match.

Combining SIM Authentication with Knowledge and Biometrics

SIM-based authentication becomes even stronger when paired with additional authentication factors such as local biometrics knowledge. The SIM confirms the device, and the identity tied to it. Biometrics confirms the person using the device at that moment. Together, they create a clear and secure picture: a trusted user, on a trusted device.

This approach avoids the usual weaknesses of biometric systems. Instead of syncing passkeys across devices or falling back to PIN codes, the SIM stays bound to a single device and network identity. Biometrics act as a local check - not the primary proof of identity, but a second layer of protection.

It also keeps sensitive data on the device. There's no need to store or transmit biometric data elsewhere. That reduces exposure and strengthens privacy.

By combining something you have (the SIM) with something you are (biometrics), authentication becomes both user-friendly and hard to break. It supports fast access without lowering security.

U.S. – The National Institute of Standards and Technology (NIST), in its SP 800-63-3 guidelines, defines three levels of authentication assurance. Similarly, the European GDPR and PSD2, along with other jurisdictions, enforce comparable authentication requirements.

- AAL1: Allows single-factor authentication; considered low assurance.
- AAL2: Requires multi-factor authentication (MFA) using two distinct factors.
- AAL3: The highest assurance level. Requires MFA with a hardware-based authenticator and resistance to verifier impersonation.

Authenticator Assurance Level 3 introduces a critical concept to defend against social engineering: Authentication Intent.

This means that when a user approves an authentication request, they are clearly informed of what they're authorizing. For example, a fraudster might call a victim pretending to be their bank and ask them to read back a generic OTP received via SMS, claiming it's part of a system test. What the victim doesn't realize is that the OTP is actually being used to activate their credit card on the fraudster's digital wallet.

SIM-based authentication not only confirms device possession, knowledge, and even biometrics—it also secures Authentication Intent by presenting a clear, secure popup on the user's phone, making the purpose of the authentication action unmistakable.

A Simpler Path to Privacy and Compliance

SIM-based authentication works without collecting behavioral or contextual data, and it doesn't require tracking how users interact with apps or websites. The SIM ID is a fixed, hardware-based identifier — stable, private, and contained within the device.

Because it avoids gathering personal signals like location, device use, or browsing patterns, SIM-based authentication sidesteps many of the complications tied to privacy regulations. There's less need for user consent flows, data governance processes, or retention policies that manage high-risk information.

This simplifies compliance. With less personal data moving through systems, the risk of a breach drops — and so does the burden of audits, reviews, and legal oversight.

By reducing reliance on sensitive data, SIM-based authentication supports both strong security and responsible data use. It delivers identity assurance without creating new risks — or new compliance costs.

The Bottom Line

Probabilistic authentication is built on guesswork. It relies on patterns, predictions, and signals that can be copied, faked, or manipulated. It depends on collecting sensitive data, adds complexity, and leaves too much room for error - especially as fraud tactics evolve. Biometrics help with convenience, but they confirm access to a device, not the identity of the user.

SIM-based authentication removes the uncertainty. It uses a fixed, tamper-proof identifier tied to the mobile network. It cannot be cloned, shared, or bypassed. It does not rely on user behavior or tracking, and it does not require fallback methods that weaken security.

As the demands on identity systems grow - from both attackers and regulators - deterministic authentication offers a better way forward. SIM-based authentication is precise, private, and built to resist the gaps that other methods can’t avoid.

Last but not least, most people could leave home with only their phone—but not without it. Every one of the 7 billion+ phones in the world operates with either a SIM or eSIM, making the SIM the most ubiquitous and reliable system for authenticating users on the go and throughout their digital journeys.

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