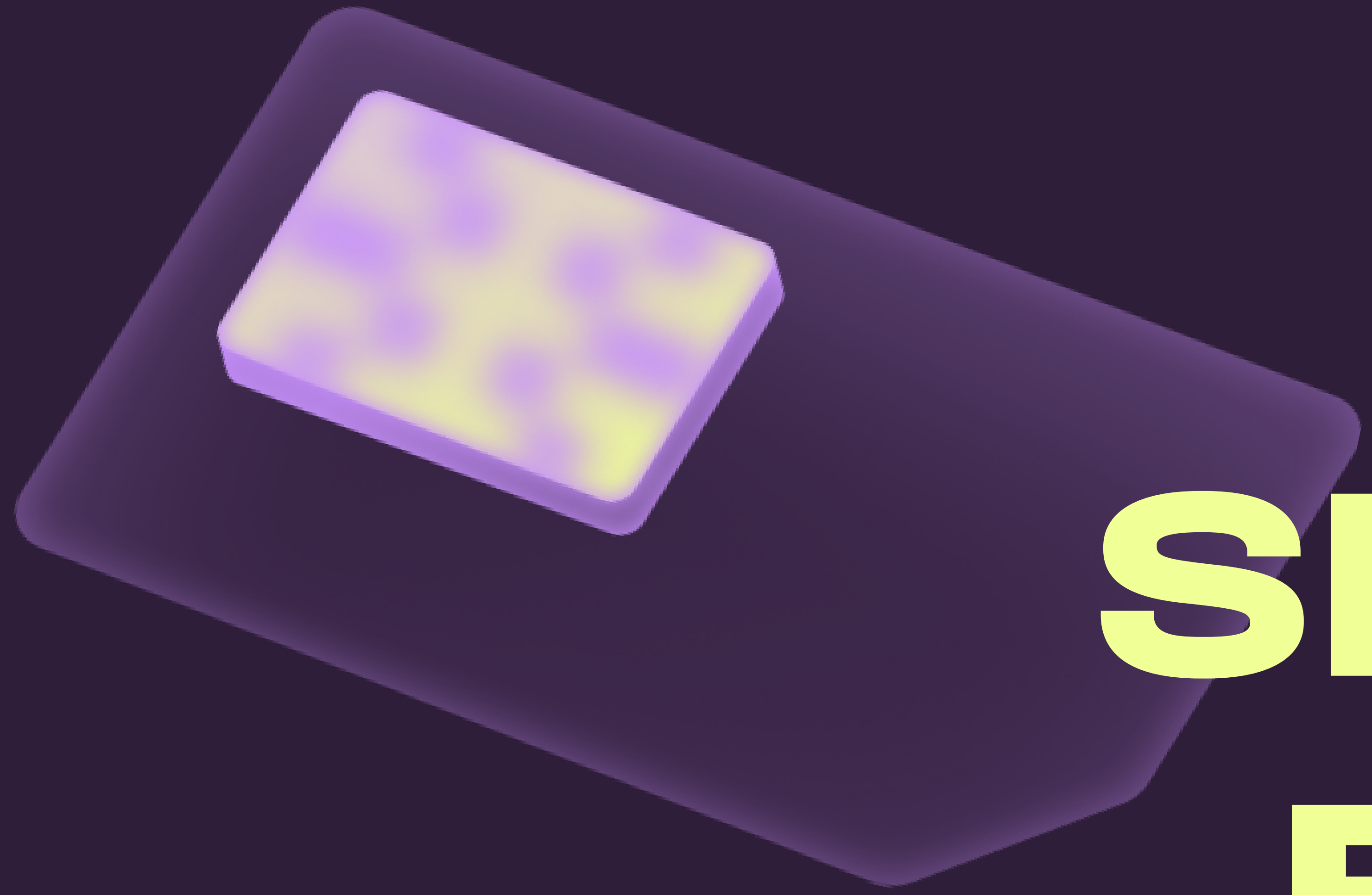
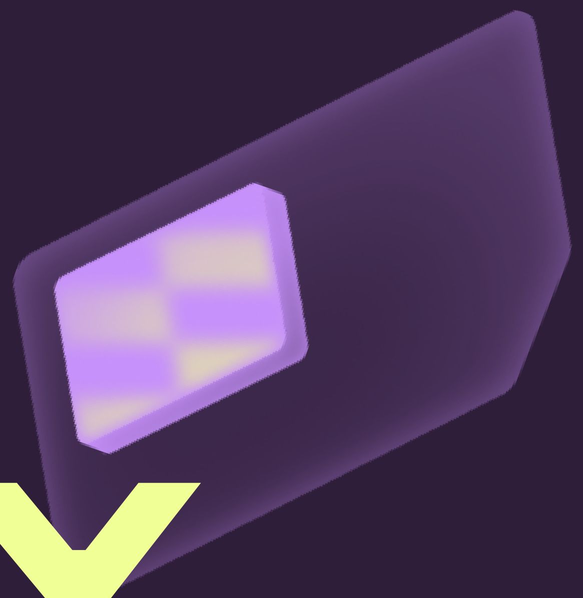
UNIBEAM





SECURITY BEYOND BIOMETRICS

How SIM-based authentication extends biometrics for user verification

A Unibeam E-Book
October 2024

Contents

The Need for Accurate User Verification

Online is the standard in the day-to-day operations of almost every enterprise. You manage data online. Nearly all customers, employees, third-party service providers, and other transactions are conducted online. This makes verifying the identity of users in your online activity—from online banking to employee work hours reporting and everything in between—a strategic security must-have.

User verification is the cornerstone of secure online interactions. By accurately confirming user identity at scale, you reduce the risk of imposters accessing sensitive information or systems. This is even more critical in sensitive sectors like finance, healthcare, and e-commerce - where unauthorized access can have serious financial and reputational consequences.

What's more, effective identity verification has become mission-critical for regulatory compliance. User data protection regulations like GDPR, HIPAA, CCPA, and others keep getting stricter. And the penalties for noncompliance are getting more severe, too. Implementing robust identity verification helps your enterprise demonstrate a commitment to compliance… and possibly avoid fines and sanctions.

Biometrics – A Secure Foundation, But...

Currently, there are three common models for user identity verification:

Knowledge-based authentication

Asking users to provide answers to security questions that only they should know

Multi-factor authentication (MFA)

Combining multiple verification factors like passwords, one-time passwords (OTPs), security tokens, and more

Biometric authentication

Using unique user physical characteristics, such as fingerprints or facial recognition, to verify identity

From smartphones to high-security military facilities, biometric authentication is considered the gold authentication standard. And it is indeed a robust foundation for authentication. Yet, while biometrics offers both convenience and security benefits, it is not without risk. Fingerprints, facial recognition, and iris scans can be compromised through, spoofing and social engineering – and not all methods work on all devices.

Biometric spoofing attacks have surged by some 50% in recent years, leading security-centric organizations to examine their biometrics programs more closely. For example, a recent US Department of Defense (DoD) report revealed significant internal biometric data security and management gaps.

This is why companies like yours are actively looking for new paradigms to verify users- augmenting biometric authentication seamlessly. SIM-based authentication – leveraging the unique identifier associated with a user's SIM card to verify their identity – is emerging as a force multiplier for traditional biometrics.

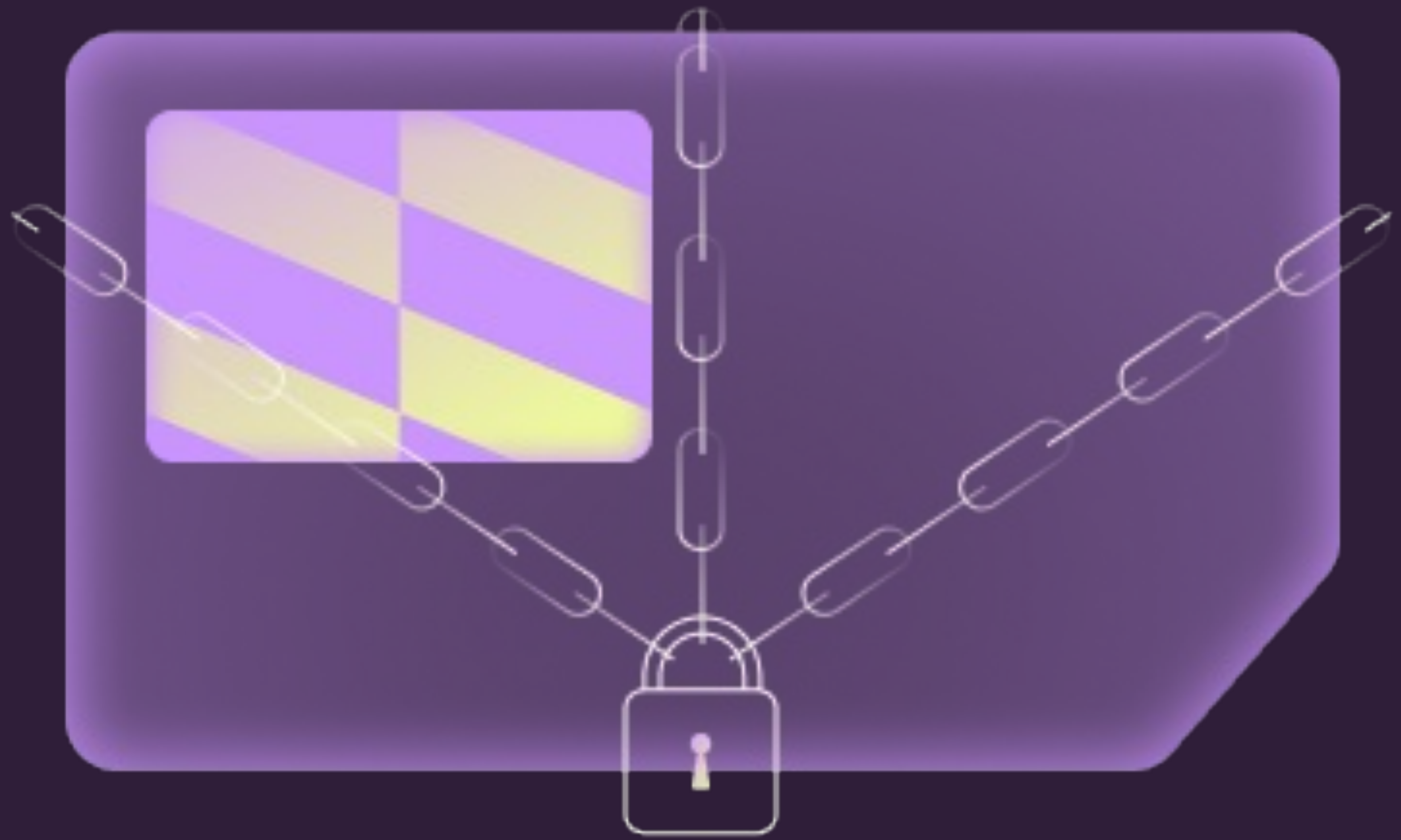
SIM Based Authentication: Maximizing Value

SIM-based user identity authentication makes biometrics-based user identity verification systems stronger – simply and cost-effectively.

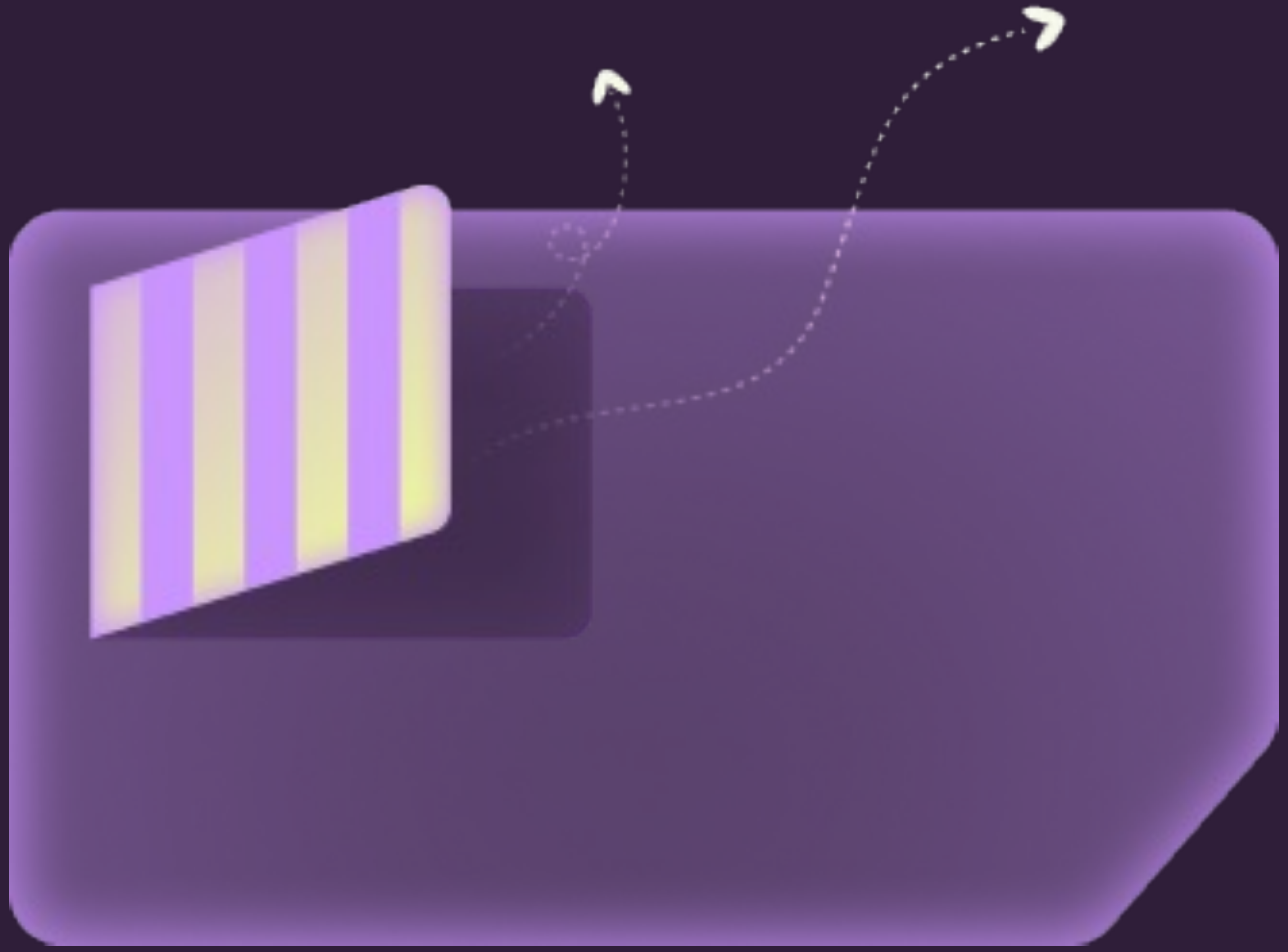
How does it work?

SIM-based authentication uses the unique identifiers associated with a user's SIM card and device to authenticate their identity – maximizing value by adding security without adding hardware.

A SIM-based user identity authentication system links the user's identity to their specific device and SIM card. This ensures that user engagement is always valid. Why? If the SIM, the device, or the number changes (because of a SIM swap or a device change), the system can detect it. Then, your system can safely block automated log-ins and redirect your users for further verification.



SIM-Based Authentication and Biometrics: A Force Multiplier



Combining SIM-based authentication with biometrics creates a powerful additional layer of security. SIM cards are physical elements, making them difficult to replicate or compromise, while biometrics are unique biological characteristics that are difficult to forge. By combining these two methods, enterprises can create a highly resilient, attack-resistant, multi-factor authentication regime.

For example, if a hacker manages to spoof biometric data representation from the phone, he or she would still need to acquire a physical SIM card to gain access. On the flip side, if a hacker gets hold of a SIM card, he or she would still need to provide the correct biometric information to authenticate.

The fusion of SIM-based and biometric authentication creates a highly secure and user-friendly authentication system that can significantly reduce the risk of unauthorized access and data breaches, making it a powerful force multiplier for enterprise security.

A World of Benefits

The fusion of SIM-based and biometric authentication creates a powerful solution that enhances enterprise security and improves the user experience. This combination creates a robust, versatile, and user-friendly authentication system that delivers:

Enhanced security through layered authentication

Joint SIM/Device and biometrics-based authentication enhances security by creating a dual-layer approach. Even if a biometric system is compromised, the second secure channel provides a fallback, significantly hindering unauthorized access.

SIM-based authentication can mitigate these limitations by offering a consistent and reliable secondary verification method. This ensures that users who cannot be accurately authenticated biometrically can still be securely verified.

Broader reach: ubiquitous and device-agnostic

By combining SIM-based and biometric authentication, enterprises enjoy a security solution that is both ubiquitous and device-agnostic. While biometric authentication may be limited to certain devices, a SIM-based approach operates independently of the device's operating system. This ensures compatibility across a wide range of devices, including legacy systems that may not support advanced biometric technologies.

This dual-layer approach provides a consistent security layer across all user devices, regardless of their capabilities. This broadens the reach of security, ensuring that users can access sensitive information and systems safely, even on older or less sophisticated devices.

More user friendly

By combining SIM-based and biometric authentication, enterprises can create a more user-friendly identity verification and authentication experience. SIM-based authentication is particularly convenient as it doesn't require any additional registration or app downloads. In many cases, it operates seamlessly in the background without requiring active user engagement.

Seamless integration with multimodal biometric systems

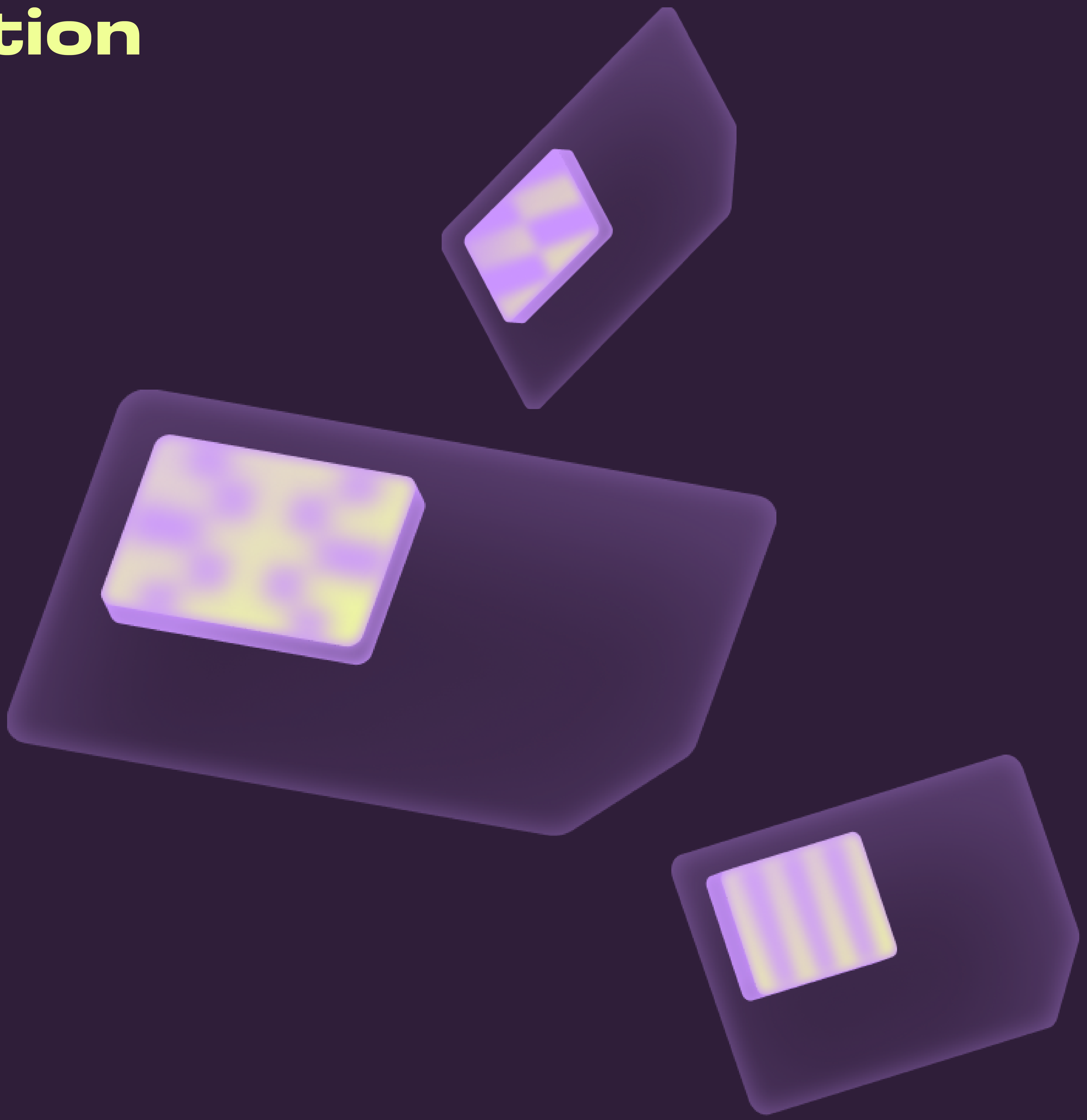
As biometric authentication evolves, multimodal systems that combine multiple biometric traits – like fingerprint, facial recognition, and voice - are required to ensure ironclad security. Unibeam’s SIM-based authentication seamlessly integrates with these advanced systems, offering an additional layer of verification that complements whatever biometric modalities are in use.

A New Era of Identity Verification

Accurate identity verification is a strategic must-have for your enterprise. It safeguards against unauthorized access, fraud, and data breaches. And it also helps ensure your compliance with stringent data protection regulations.

Biometric authentication, while a powerful tool, has limitations. SIM-based authentication is a valuable complement to biometric systems – adding a robust and seamless additional layer of security.

Solutions combining SIM-based and biometric authentication are versatile and user-friendly. As your organization works to navigate digital complexities, the fusion of SIM-based and biometric authentication can play a crucial role in keeping your assets safe, protecting your customer data, and ensuring your business continuity.



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.

UNIBEAM