WWW.SECUROSYS.COM

SASE & HSM: STRENGTHENING CLOUD SECURITY ONE KEY AT A TIME

securosys

EXECUTIVE SUMMARY

The cloud is redefining modern IT infrastructure, driving innovation in cloud-native applications and enabling hybrid workforces with flexible, secure access. But as the cloud expands, so does the attack surface. To address these challenges, many organizations are turning to SASE (Secure Access Service Edge) — an elegant, unified service model combining networking and security into a single framework.

One critical element, however, is often overlooked in the SASE conversation: strong key management. Without it, encrypted traffic is only as secure as the place you store your keys. That's where Hardware Security Modules (HSMs) come in. Whether deployed on-premises or as cloud service, HSMs safeguard encryption and signing keys in certified, tamper-resistant environments.

This white paper explores how HSMs complement SASE architectures, ensuring that the data security perimeter extends all the way to the keys, because without protected keys, there is no real encryption.

securosys

THE WORLD IS RACING INTO THE CLOUD

Hybrid work is here to stay, cloud-native apps are the new standard, and perimeter-based security just doesn't cut it anymore. Security must follow users, apps, and data — wherever they are. That's exactly what SASE is designed to do.
SASE combines once-separate disciplines, networking (like SD-WAN and routing) and security (like firewalls, secure web gateways, and zero trust frameworks), into a single, cloud-delivered service model.

But there's a missing link: where and how encryption keys are managed. Without strong, hardware-based key protection, even the most advanced SASE architecture remains vulnerable.

securosys

HSM & SASE: A PERFECT COMBINATION

1

SECURING ENCRYPTION KEYS INSIDE THE SASE CLOUD

HSMs keep encryption keys safe in certified hardware — not exposed in software-only systems or uncontrolled third-party environments.

2

ZERO TRUST STARTS WITH STRONG AUTHENTICATION

Zero Trust relies on certificates and private keys. Storing these in HSMs prevents exposure, securing identity credentials used across users, devices, and sessions.

3

REPLACING VPNS WITH TLS — AND PROTECTING TLS KEYS

SASE uses TLS to replace legacy VPNs, but TLS keys are prime attack targets. HSMs ensure these keys can't be extracted, even if management layers are compromised.

4

CASB: ENCRYPTION AT REST NEEDS KEY PROTECTION

CASBs encrypt data in SaaS platforms, but the protection is only as strong as the key storage. HSMs enforce hardware-based control over who can decrypt or sign data.

5

COMPLIANCE WITH SECURITY REGULATIONS

Regulatory frameworks demand strong encryption and key management. HSMs provide a clear, certifiable answer to the critical question: "Where are the keys?"

In more details...

SECURING ENCRYPTION KEYS INSIDE THE SASE CLOUD

SASE handles vast amounts of encrypted traffic — between users, cloud apps, edge services, and branch offices. But if the keys that protect this traffic are stored in software-only systems or third-party cloud environments, the entire security posture is weakened.

HSMs close this gap. Whether deployed on premises or via georedundant CloudHSM, encryption keys remain within certified, tamper-proof hardware, under your control. You get cloud flexibility without losing cryptographic sovereignty.

ZERO TRUST STARTS WITH STRONG AUTHENTICATION

Zero Trust requires continuous identity verification. That means a reliance on digital certificates and private keys. Storing these sensitive keys in software risks exposure.

By managing your PKI infrastructure within an HSM, you protect private keys used for endpoint identity, client certificates, and secure tunnels — ensuring they're never exposed outside the HSM.

REPLACING VPNS WITH TLS — AND PROTECTING TLS KEYS

SASE replaces legacy VPNs with scalable TLS-based access. But TLS private keys and certificates are prime targets. If stolen, attackers can decrypt traffic or impersonate your services.

HSMs store these keys securely, ensuring they can't be extracted even if your SASE management console is compromised. The result: secure access without weak links.

CLOUD ACCESS SECURITY BROKERS (CASB): ENCRYPTION AT REST

Many SASE frameworks include CASBs to secure cloud like Salesforce, or Workday. CASBs encrypt sensitive fields inside these apps — but the strength of that encryption relies on where keys are stored.

With HSMs, encryption keys remain hardware-protected, ensuring only authorized operations like decryption or signing are permitted, and only by authorized parties.

securosys

COMPLIANCE WITH SECURITY REGULATIONS

Whether it's GDPR, HIPAA, or DORA, regulators expect strong key protection, auditability, and data sovereignty. A SASE solution may encrypt traffic — but authorities want to know: where are the keys?

With Securosys HSMs (on-prem or CloudHSM), you have a certified, auditable answer that satisfies the highest compliance standards — and keeps you in full control.

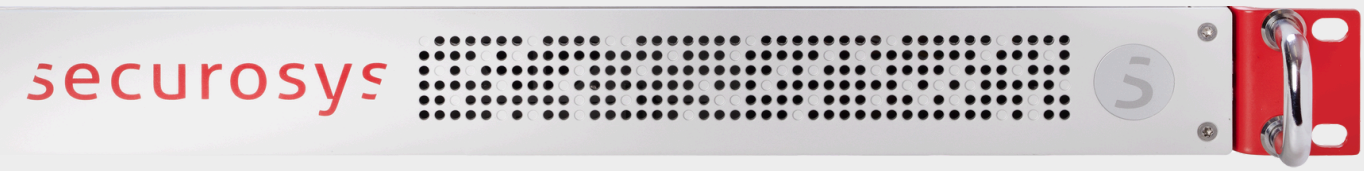
USE CASES

CLOUD SERVICE PROVIDERS

Cloud providers delivering SASE can embed CloudHSM into their platforms, offering enterprise clients an optional — yet essential — security upgrade: full control over their cryptographic keys, even in multi-tenant environments. Geo-redundant CloudHSM clusters ensure resilience and global scale.

FINANCIAL SERVICES

Banks, FinTechs are moving to cloud-native SASE for performance and agility. But compliance and key security are non-negotiable. Whether signing transactions or encrypting customer data, integrating HSMs ensures that critical cryptographic materials never leave secure hardware, meeting the highest standards for integrity and trust.



CONCLUSION

SASE secures your network. HSM secures your keys. Together, they provide an end-to-end security architecture capable of withstanding today's advanced threats and tomorrow's regulatory audits.

With Securosys HSM — available as CloudHSM or on-prem — you gain all the advantages of modern, scalable, cloud-native security without compromising on cryptographic control.

Want to learn more about how CloudHSM can enhance your security infrastructure? Contact us!

WWW.SECUROSYS.COM/CONTACT

ABOUT US

Securosys SA, headquartered in Zurich, Switzerland, is a renowned industry leader specializing in cybersecurity, encryption, as well as digital identity and online keys protection. Founded in 2014, Securosys' hardware security modules (HSMs) secure transactions exceeding 100 billion euros daily on the Swiss banking system SIC (under the supervision of the Swiss National Bank) as well as the Swiss stock exchanges SIX and SDX. Over half of the world's Tier 1 banks and numerous technology companies trust the HSMs developed and manufactured by Securosys in Switzerland.

Securosys' comprehensive HSM solutions, available both on-premises and as a service in the cloud, are certified to the highest security standards, including FIPS and Common Criteria. Designed for diverse industries including finance, healthcare, and government, Securosys HSMs offer unparalleled features such as independent, cryptographically secure partitions, patented policy-based individual key protection, and cloud readiness. The devices support hybrid signatures, ensuring a seamless transition from classical to post-quantum cryptographic (PQC) algorithms.