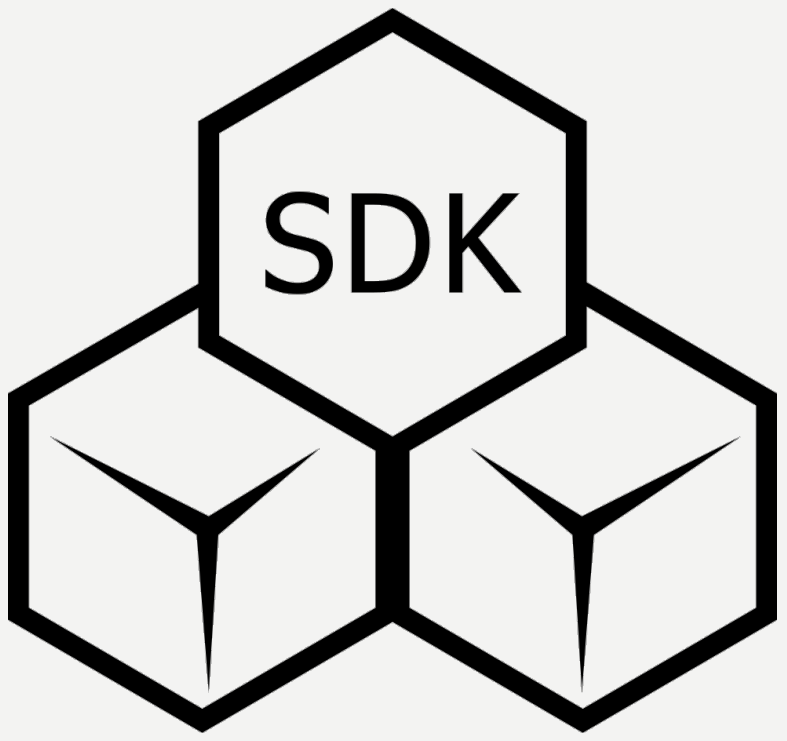
XSOC SDK DEPLOYMENT GUIDE



XSOC SDK DEPLOYMENT GUIDE:
MINIMUM HARDWARE AND SYSTEM REQUIREMENTS

The XSOC Cryptosystem SDK is designed to deliver high-performance, AIDA-proof encryption with minimal system overhead. It offers a lightweight implementation that can run efficiently across a variety of environments, from enterprise servers to IoT edge devices. Below are the minimum hardware and software requirements for deploying the XSOC SDK in different operational environments.

1. GENERAL DEPLOYMENT REQUIREMENTS

XSOC SDK is highly adaptable and can be deployed on a variety of systems with minimal computational footprint. It does not require specialized cryptographic hardware and functions entirely in software, ensuring flexibility for developers and enterprise architects.

Minimum System Requirements

Component	Minimum Requirement	Recommended Requirement
CPU	1 GHz dual-core (x86_64, ARM)	2.5 GHz quad-core (x86_64, ARMv8)
RAM	512 MB	4 GB
Storage	50 MB free space	200 MB free space
OS Compatibility	Windows (10, 11, Server 2016+), macOS, Linux (Ubuntu, CentOS, RHEL, Debian), Android, Embedded OS (Yocto, RTOS)	Same as minimum, with enterprise-grade Linux preferred
Virtualization	Compatible with Docker, Kubernetes, VMware, Hyper-V	Dedicated bare-metal preferred for maximum performance
Networking	Standard TCP/IP Stack	Supports LAN, WAN, VPN, and Encrypted Broadcast Protocol (EBP)

2. CLOUD & VIRTUALIZED ENVIRONMENTS

XSOC is optimized for deployment in cloud-native architectures, including hybrid and on-premise configurations.

Cloud Provider	Supported Environments
AWS	EC2, Lambda, ECS, EKS, S3 (encrypted with XSOC)
Microsoft Azure	Virtual Machines, Azure Functions, Kubernetes Service
Google Cloud	Compute Engine, Cloud Functions, Kubernetes
IBM Cloud	Bare Metal, VPC, Kubernetes
Oracle Cloud	Compute, Autonomous DB, Exadata

Note: XSOC provides hardware-agnostic encryption and can integrate with KMS and HSM solutions while offering post-quantum cryptographic resilience.

3. ON-PREMISE & ENTERPRISE SERVER DEPLOYMENTS

For high-performance on-premise or private cloud installations, XSOC SDK can be deployed on standard server-grade infrastructure.

Component	Minimum Requirement	Recommended Requirement
Processor	Intel Xeon E3 / AMD EPYC	Intel Xeon Platinum / AMD EPYC Milan
Memory	8 GB DDR4 ECC	32 GB DDR5 ECC
Storage	SSD (NVMe preferred)	RAID-10 SSD/NVMe
Network	1 Gbps Ethernet	10 Gbps Ethernet / Fiber
Security Modules	TPM 2.0 (Optional)	FIPS-140-3 Certified HSM (Optional)

Performance Impact: XSOC encryption operates with near-zero latency, making it ideal for high-frequency financial transactions, large-scale data encryption, and mission-critical workloads.

4. EDGE & IOT DEVICE DEPLOYMENTS

XSOC SDK is optimized for low-power, constrained environments, enabling secure encryption in edge computing and IoT applications.

Device Type	Minimum Requirement
Raspberry Pi 4	2 GB RAM, 1.5 GHz ARM Cortex-A72
Embedded Devices	ARM Cortex-M7, MIPS64, RISC-V 64-bit
IoT Gateways	Dual-core ARM Cortex-A53, 512 MB RAM
SCADA Systems	x86 or ARM 64-bit CPU, RTOS/Linux support

Integration: XSOC SDK runs efficiently on embedded and real-time operating systems (RTOS), ensuring robust cryptographic security for industrial and operational technology (OT).

5. DEPLOYMENT & INTEGRATION CONSIDERATIONS

XSOC SDK supports multiple development environments, programming languages, and integration methods.

Feature	Compatibility
Programming Languages	Java, C, C++, Rust, Python, Go
Deployment Modes	JAR file, Docker, Static/Dynamic Library, API-based
PKCS#11 Compliance	Fully supported
Key Management	Native XSOC Key Store, External HSM, KMS (AWS KMS, Azure Key Vault, HashiCorp Vault)
Authentication	XSOC HyperKey (MFA), FIDO2, TPM-backed security
Streaming Encryption	Perfect Forward Secrecy (PFS), Ephemeral Key Exchange

6. PERFORMANCE BENCHMARKS

XSOC outperforms traditional encryption algorithms while maintaining a minimal system footprint.

Encryption Algorithm	Throughput (MB/s)	Latency (ms)
AES-256 (Software)	300-400 MB/s	~3.5 ms
ChaCha20-Poly1305	450-600 MB/s	~2.8 ms
XSOC (Software, Java)	1200+ MB/s	~0.8 ms
XSOC (Optimized C/Rust)	1800+ MB/s	~0.5 ms

Comparison: XSOC achieves **4-6x faster encryption** than AES-256 while running purely in software without hardware acceleration.

7. SECURITY & COMPLIANCE

XSOC is built with **post-quantum resistance** and **AIDA-proof security** to protect against modern cryptographic threats.

Compliance Standard	XSOC Compliance
FIPS 140-3	Fully validated
NIST PQC Transition Plan	Compatible
GDPR, CCPA, HIPAA	Meets encryption requirements
ISO 27001, SOC 2	Supports secure integration

The XSOC Cryptosystem SDK is a **lightweight, high-performance encryption engine** that is designed for **cloud, enterprise, IoT, and embedded systems**.

With **sub-millisecond initialization, ultra-low system overhead, and scalability across diverse computing environments**, XSOC delivers cutting-edge cryptographic security without impacting performance.

Our post-quantum resilience and AIDA-resistant architecture make it the ideal security framework for modern cybersecurity challenges.