Solution Guide

Supply Chain Security Assurance

Introduction

At ZPE Systems, we take the security of our supply chain very seriously. While we do not publicly disclose specific details about the members of our supply chain, we ensure that every step of our product lifecycle—whether it involves hardware, software, or cloud offerings—is safeguarded through a comprehensive, layered security approach. We strictly adhere to compliance with government regulations, including any restrictions on the use of technology by enterprises due to regulatory mandates.

ZPE Systems Value Chain Security

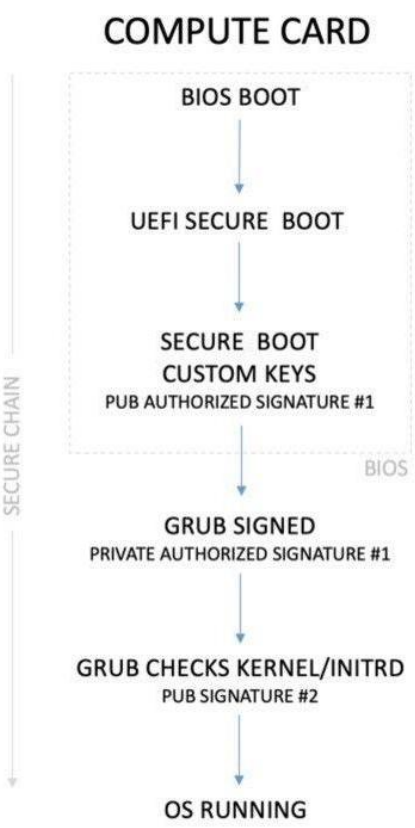
Our value chain security is designed with the following key objectives:

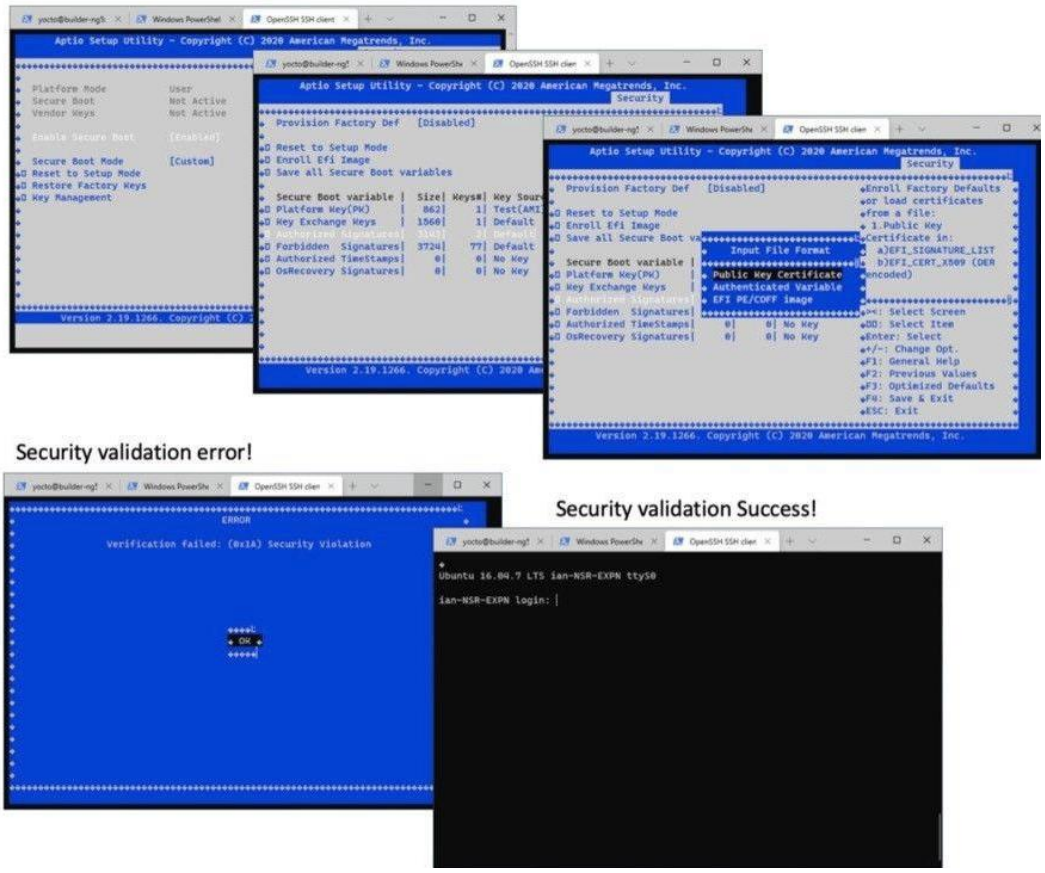
- **Secure Development, Manufacturing, and Deployment:** ZPE Systems solutions are developed, manufactured, and deployed within securely controlled environments. We use only ZPE Systems-approved processes, tools, and components throughout these stages to ensure the integrity of our solutions.
- **Prevention of Malware and Rogue Materials:** Our processes are designed to prevent the introduction of any malware or unauthorized raw materials that could compromise the functionality of our products.
- **Counterfeit Prevention:** Our build and deployment processes are structured to make it extremely difficult for malicious actors to produce counterfeit solutions. By securing every stage of development, we protect our products from being altered or replicated in unauthorized ways.

Hardware Security

ZPE Systems' hardware security features are integral to our supply chain assurance, providing robust protection against tampering and unauthorized access:

- **TPM Trusted Platform Module:** Our hardware includes TPM 2.0, which provides hardware-based security functions, including secure key generation and storage. This module ensures that only authenticated software can run on our devices.
- **UEFI Boot with Signed OS:** We enforce the use of UEFI Boot with Signed OS, which prevents the execution of unauthorized software during the boot process, safeguarding the integrity of the system from the very start.
- **Password Protected Boot and BIOS**: To further protect against unauthorized access, our devices require passwords for both boot and BIOS access, adding another layer of security.
- **Secure Erase:** This feature allows for the secure deletion of all data from storage devices, ensuring that no sensitive information remains recoverable.
- **Self-Encrypting Drive (SED)**: Our solid-state drives (SSDs) feature hardware-based encryption, protecting data at rest without sacrificing performance.
- **Device Certificate in TPM Module:** Each device is equipped with a certificate within the TPM module, which identifies the hardware as a genuine ZPE device, preventing counterfeiting and ensuring authenticity throughout the supply chain.





Software Security

ZPE Systems employs a comprehensive approach to software security that spans the entire software development lifecycle, ensuring that our supply chain remains secure and resilient:

- **Supply Chain 3rd Party Validation:** We use a combination of static analysis, dynamic analysis, and software composition analysis to cover a wide range of potential vulnerabilities. This multi-layered approach ensures that code quality and security issues are identified at various stages of development and across different types of code.
    - **Synopsys Coverity®:** This tool allows us to identify critical quality defects and security vulnerabilities early in the development process, when they are easiest to fix. By integrating Coverity into our CI/CD pipelines, we maintain secure, high-quality applications.
    - **Synopsys WhiteHat™ Dynamic**: As a dynamic application security testing solution, WhiteHat Dynamic enables us to quickly scale our web security program. It provides continuous vulnerability assessments of applications in both QA and production environments, mimicking techniques used by malicious actors. This allows us to prioritize vulnerabilities and streamline the remediation process.
    - **Synopsys Black Duck®:** Black Duck is critical for managing supply chain security and license risks, especially in cases where we don't have access to the underlying software's code. It helps us generate a complete Software Bill of Materials (SBOM), which tracks third-party and open-source components and identifies known security vulnerabilities, associated licenses, and code quality risks .
- **Zero Critical CVE Policy:** We maintain a strict policy of zero critical Common Vulnerabilities and Exposures (CVEs). Any critical CVEs identified in third-party libraries are immediately addressed and fixed, ensuring that our software remains secure and resilient against emerging threats.

Third-Party Certifications

ZPE Systems' commitment to supply chain security is further validated by our adherence to the following industry-recognized certifications:

- **FIPS 140-2 and FIPS 140-3 Compliance:** Our products comply with these federal standards, which certify the security of cryptographic modules.
- **PCI-DSS Compliance:** We meet the Payment Card Industry Data Security Standard (PCI-DSS) requirements, ensuring that our solutions protect sensitive payment data.
- **SOC 2 Type 2** Certification: This certification demonstrates our commitment to maintaining stringent security, availability, and confidentiality controls across our systems.
- **ISO 27001 Certification:** Our information security management system is certified to the ISO 27001 standard, reflecting our commitment to robust security practices across our organization.

Conclusion

ZPE Systems is dedicated to maintaining the highest standards of security across our supply chain.

From hardware to software and cloud offerings, every aspect of our product lifecycle is designed with security in mind.

Our layered security approach, rigorous testing processes, and adherence to industry certifications ensure that our customers can trust the integrity and reliability of our products, knowing that they are protected from the risks of an increasingly complex threat landscape.

For further information or to discuss our supply chain security practices, please contact **info@zpesystems.com**

Automation Infrastructure Solution Comparison

Vendors	Gen3 OOBI	OOBI-WAN and Security	Platform & Tools	Management	
				On-Prem	SaaS
ZPE Systems	●	●	●	●	●
Vendor A	◕	◑	◔	●	○
Vendor B	◑	◔	○	◑	○
Intel NUC/Whitebox	○	○	●	○	○

Security in Layers

		ZPE Systems	Others
Security Integrations	• CyberArk, Delinia, Horizon3.ai • PaloAlto, Fortinet, Cloudflare	✓ ✓	○ ○
Certification and Processes	• SOC2 Type 2, FIPS140-3, • PSIRT, Pentesting	✓ ✓	○ ○
Software & Cloud	• Latest Kernel and CVE patches • Zero Trust based access • SAML2 based SSO • MFA • Latest encryption standards	✓ ✓ ✓ ✓ ✓	○ ○ ○ ○ ○
Software Development	• Dynamic Code Analysis • Static Code Analysis • Software BOM analysis including Open Source Software Composition • Continues Security Assessments • Zero CVE Policy • Vulnerability Scan	✓ ✓ ✓ ✓ ✓	○ ○ ○ ○ ○
Hardware	• Secure Signed OS • Password-protected BIOS and Boot Loader • TPM 2.0 • Self Encrypted Disk • Secure Boot • Geo Fencing Protected	✓ ✓ ✓ ✓ ✓ ✓	○ ○ ○ ○ ○ ○

Synopsys Coverity Validated · Synopsys BlackDuck Validated · Synopsys Whitehat Validated · SOC 2 TYPE II CERTIFIED · Qualys. · FIPS 140-3

Additional Resources:

- Nodegrid OS Security Considerations
- ZPE Cloud Security Considerations
- Synopsys - ZPE Systems Case Study
- Vulnerability Disclosure Policy

Certifications

- ISO/IEC 27001:2022
- Vulnerability Disclosure Policy
- FirstNet Certification
- TAA Compliance
- FIPS 140-3
- PCI DSS Compliance
- SOC 2 Type 1
- SOC 2 Type 2