Silicon-First Security with PSA Certified: Building Trust in Connected and Non-Connected Digital Devices from the Chip Up

PSA Certified provides a structured framework for implementing and validating security at the silicon level, creating a foundation of trust that extends throughout a device's lifecycle. For any device with digital functionality (software/hardware that processes data or runs code), whether connected to networks or completely isolated, security must begin at the chip level. This paper explains how PSA Certified helps manufacturers build devices that are secure by design and compliant with evolving global regulations, making the case for a silicon-first approach to cybersecurity that protects all digital products.

Table of Contents

Introduction: The Hidden Security Challenge of Digital Devices 1

Regulatory Pressure and Compliance Requirements 2

Why Security Must Start with Silicon 3

Real-World Security Breach Examples 4

Understanding PSA Certified 5

The PSA Certified Assurance Levels 7

The PSA Root of Trust Architecture 10

Implementing PSA Certified in Product Design 12

EnSilica's Approach to PSA Certified 13

Conclusion: Building Trust from the Silicon Up 15

Introduction: The Hidden Security Challenge of Digital Devices

The proliferation of digital technology means that virtually every sector now relies on devices that process data or execute code, from industrial automation and healthcare to automotive and consumer electronics. While much of the cybersecurity conversation centres around internet-connected products, the reality is that any device with embedded digital components can be a target, even if it never connects to a network.

Digital elements, whether in isolated medical equipment, transportation controls, or critical infrastructure, can be exploited if not properly secured. This expanded digital footprint increases the number of potential entry points for attackers. As a result, the foundation of device trust must be established at the hardware level, regardless of whether the device is online or offline.

The PSA Certified framework, developed to address these challenges, provides a structured approach to building secure devices from the ground up. For systems engineers and chip architects, this means integrating security into the earliest stages of design, rather than treating it as an afterthought or relying solely on software-based protections.

Regulatory Pressure and Compliance Requirements

Legislators and regulatory bodies around the world are responding to the growing complexity and risk of digital products by introducing new cybersecurity mandates. These regulations are designed to ensure that security is integrated throughout a product's lifecycle, from initial design through to end-of-life.

Key regulatory frameworks include:

- **EU Cyber Resilience Act (CRA)[1]:** This regulation applies to all products with digital elements, requiring security-by-design, secure update mechanisms, and a minimum five-year support window. It also enforces supply chain accountability, mandating that vendors ensure their third-party components meet the same standards. Full enforcement is set for December 2027.
- **UK Product Security and Telecommunications Infrastructure (PSTI) Act[2]:** The PSTI Act requires manufacturers, importers, and distributors to declare update timelines, implement robust vulnerability disclosure processes, and comply with standards such as ETSI EN 303 645 or ISO/IEC 29147. Penalties for non-compliance can reach £10 million or 4% of global turnover, with additional daily fines for ongoing violations.
- **EU Radio Equipment Directive (RED)[3]:** From August 2025, this directive mandates compliance with EN 18031 for wirelessly connected devices, ensuring network protection, fraud resistance, and personal data privacy.
- **US Cyber Trust Mark[4]:** While currently voluntary, this mark is becoming a de facto standard for federal procurement, requiring alignment with NIST 8259A/B and 8425. This trend is mirrored in other regions, including China's GB/T 36951 and evolving frameworks in Singapore and Australia.

[1] European Commission. *Cyber Resilience Act*. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

[2] UK Government. *Product Security and Telecommunications Infrastructure Act Guidance*. https://www.gov.uk/guidance/regulations-consumer-connectable-product-security

[3] European Commission. *EU Radio Equipment Directive (RED) - 2014*. https://single-market-economy.ec.europa.eu/sectors/electrical-and-electronic-engineering-industries-eei/radio-equipment-directive-red_en

[4] FCC. *Cyber Trust Mark Initiative*. https://www.fcc.gov/CyberTrustMark

For manufacturers, this means that products intended for international markets must meet a diverse set of requirements. Adopting a unified, standards-based approach to security not only simplifies compliance but also builds customer trust and competitive advantage.

In today's regulatory landscape, demonstrating compliance is not just about avoiding penalties; it is essential for market access and brand reputation.

Why Security Must Start with Silicon

When security is implemented at the chip level, it establishes a Root of Trust that cannot be compromised by software vulnerabilities or malicious code. This hardware-based security foundation provides several critical advantages:

1. **Immutability**: Hardware-based security features cannot be altered or bypassed by software attacks, creating a stable foundation for the security architecture.
2. **Performance Efficiency**: Security functions implemented in hardware typically operate more efficiently than software-based alternatives, with lower power consumption and higher throughput.
3. **Isolation**: Hardware-based security enables strong isolation between different system components, containing potential breaches and preventing escalation.
4. **Longevity**: Digital devices may remain in operation for 10-15 years or more. Silicon-level security ensures the ability to support secure updates, key rotation, and resilience against evolving threats throughout this extended lifecycle.
5. **Defence Against Physical Attacks**: Only hardware-based security can defend against physical tampering, side-channel analysis, and other hardware-level attack vectors.

By embedding security into the chip from the outset, manufacturers can ensure that their products are resilient to both current and emerging threats, while also simplifying the path to regulatory compliance.

Limitations of Software-Only Security

Software-based security measures, while necessary, are insufficient on their own:

- They operate on top of potentially vulnerable hardware
- They can be modified, disabled, or bypassed if the underlying system is compromised
- They may introduce performance overhead and latency
- They cannot fully protect against hardware-level vulnerabilities

The Long-Term Impact of Hardware Security Decisions

Decisions made during the chip design phase have lasting consequences throughout a product's entire lifecycle. Retrofitting security into an existing system is rarely effective and often impossible. When security is considered from the outset, manufacturers can:

- Build devices that remain secure through their entire operational life
- Support secure updates to address emerging threats
- Reduce the total cost of security by avoiding expensive remediation efforts
- Meet evolving regulatory requirements with fewer design changes
- Establish customer trust through demonstrable security practices

Real-World Security Breach Examples

Understanding real-world security breaches helps illustrate why a silicon-first approach to security is critical. These examples demonstrate that even devices without internet connectivity can be vulnerable to sophisticated attacks.

Automotive Security: Headlight Hacking[5]

In May 2024, thieves in Coventry, UK, stole a Toyota C-HR in under 30 seconds using a technique called "headlight hacking." The criminals:

1. Gained access to the vehicle's headlight assembly
2. Accessed the CAN bus wiring connected to the key receiver ECU
3. Used a device to send fake CAN frames indicating that a key had been validated
4. Bypassed the immobiliser system
5. Started and drove away with the vehicle

This attack required no internet connection but exploited weaknesses in the vehicle's internal communication architecture. A properly implemented Root of Trust at the silicon level could have prevented the injection of unauthorised commands into the system.

Air-Gapped System Breaches: GoldenJackal[6]

Between 2019 and 2024, the advanced persistent threat group, GoldenJackal, successfully compromised air-gapped government systems in Europe, the Middle East, and South Asia. Despite these systems being physically isolated from networks, the attackers:

1. Used custom malware specifically designed to evade detection
2. Introduced the malware to isolated systems, likely via USB drives

[5] The Sun. *Toyota Car Theft via Headlight Hacking – Coventry, 2024*. https://www.thesun.co.uk/motors/30879632/shocking-moment-thieves-hack-cars-headlights/

[6] The Register. *APT GoldenJackal Targeting Air-Gapped Systems – 2019-2024*. https://www.theregister.com/2024/10/09/goldenjackal_custom_malware

3. Extracted sensitive data, including emails, encryption keys, and confidential documents
4. Established covert communication channels for future attacks

This sophisticated attack demonstrates that physical isolation alone is insufficient for security. A comprehensive security approach starting at the silicon level, with secure boot, attestation, and hardware-enforced isolation, provides stronger protection against such threats.

Critical Infrastructure: Crosswalk Signals Hack[7]

In April 2025, Seattle pedestrians encountered an unusual security breach when crosswalk audio buttons were hacked to imitate Jeff Bezos's voice. The hack:

1. Modified the audio messages at several crosswalk locations
2. Replaced standard safety messages with unauthorised content
3. Demonstrated vulnerabilities in municipal infrastructure
4. Highlighted how even simple systems can be compromised

While more amusing than dangerous, this incident illustrates how embedded systems in public infrastructure can be vulnerable to tampering. Adopting PSA Certified's recommendations on secure updates and tamper resistance would help prevent such modifications.

These examples highlight the breadth of potential security threats facing digital devices, regardless of their connectivity status. They underscore the need for comprehensive security measures built from the silicon level up, as advocated by the PSA Certified framework.

Understanding PSA Certified[8]

Claiming a device is secure is no longer sufficient; manufacturers must be able to demonstrate it through verifiable evidence. PSA Certified provides a structured path to security assurance and regulatory alignment. Developed by Arm in collaboration with leading security experts, PSA Certified is a scalable, multi-level certification scheme that assesses how effectively digital products meet ten core security goals.

Since its launch in 2017, PSA Certified has grown into one of the most widely adopted global security frameworks. It was created to simplify the implementation of robust security practices by offering clear guidance, comprehensive resources, and independent, lab-based

[7] The Seattle Times. *Seattle Crosswalk Button Hack - April 2025*. https://www.seattletimes.com/seattle-news/seattle-crosswalk-signals-hacked-to-imitate-jeff-bezos-voice/

[8] PSA Certified. *Overview and Certification Levels*. https://www.psacertified.org

evaluation. This approach helps reduce complexity while enabling manufacturers to deliver products that are secure by design and ready for an increasingly regulated marketplace.

The Ten Security Goals

PSA Certified is built around ten core security goals that form the foundation for device security:

1. **Unique Identification**: Each device requires a unique identity that can be attested, facilitating trusted interactions such as data exchange and device management.
2. **Security Lifecycle**: Devices must support a security lifecycle that depends on software versions, runtime status, hardware configuration, debug port status, and product lifecycle phase. Each security state should be attestable and may impact device access.
3. **Attestation**: The device must provide evidence of its properties, including identity and security state, as part of a verification process using a trusted third party.
4. **Secure Boot**: Only authorised software should be executed on a device through secure boot and loading processes. Unauthorised boot code must be detected and prevented.
5. **Secure Update**: Secure update mechanisms are required to provide security or feature updates. Only authentic and legitimate firmware should be updated on the device.
6. **Anti-Rollback**: Prevention of rollback to previous software versions is essential to ensure that security vulnerabilities in older versions cannot be exploited. Rollback should only be possible for recovery purposes when authorised.
7. **Cryptographic/Trusted Services**: A minimal set of trusted services and cryptographic operations should be implemented as building blocks, supporting critical functions like security lifecycle, isolation, and secure storage.
8. **Isolation**: Services must be isolated from one another to prevent one service from compromising others, separating trusted services from less trusted or untrusted services.
9. **Secure Storage**: Private data must be uniquely bound to trusted services or devices to prevent cloning or unauthorised access. This typically uses cryptographic keys that are themselves bound to the device and service.
10. **Interaction**: Devices must support secure interaction across isolation boundaries without compromising the system, considering both internal device interactions and communication with the outside world.

How PSA Certification Works

PSA Certified evaluation is conducted by independent security laboratories that assess products against the framework's requirements. Certification is awarded by independent labs

and issued as a digital certificate with a unique identifier that vendors can reference in datasheets, marketing materials, and regulatory submissions.

The certification process involves different approaches depending on the level of assurance sought, ranging from questionnaire-based assessments to rigorous laboratory testing.

Benefits of PSA Certification

PSA Certified supports:

- **Accelerated Development**: It provides a trusted approach designed by security experts, speeding up the development of secure systems.
- **Market Access**: Alignment with industry and government standards helps increase access to global markets, particularly as regulations evolve.
- **Independent Validation**: The certification offers an industry-standard measurement of security implementation, validated by independent labs and third parties.
- **Customer Trust**: Certification demonstrates a commitment to security best practices, building confidence among customers and partners.

For systems engineers, PSA Certified provides a scalable, structured framework that simplifies the complex task of implementing comprehensive security while ensuring that all critical aspects are addressed.

The PSA Certified Assurance Levels

PSA Certified is structured across four levels of assurance. Each level is cumulative: achieving a higher level means meeting the requirements of the previous ones.

While Level 1 applies across three implementation layers (chip, system software, and device), Levels 2 to 4 focus exclusively on the chip, reflecting increasingly rigorous security evaluation at the hardware level.

Level 1: Foundation Security Principles

PSA Certified Level 1 demonstrates that fundamental security principles have been implemented at the chip, system software, or device level. Certification is based on a structured security questionnaire that covers secure boot, cryptographic services, secure storage, lifecycle state enforcement, and vulnerability disclosure—core elements of the PSA Root of Trust.

Vendors must support each response with technical details and documentation. An independent security lab reviews the submission, may request clarifications or additional evidence, and verifies alignment with PSA Certified's baseline threat model.

Level 1 is well-suited for consumer-grade devices or products with lower exposure to physical or network threats. Its lightweight, cost-effective approach makes it an ideal starting point for organisations beginning their security journey.

Level 2: Protection Against Software Attacks

PSA Certified Level 2 provides a rigorous, lab-based evaluation designed primarily for chip vendors. It focuses on verifying that the PSA Root of Trust (PSA-RoT) can resist scalable software attacks, including code injection, buffer overflows, privilege escalation, insecure firmware updates, and weak cryptography.

Certification requires submitting the chip and supporting documentation to an independent security laboratory. The assessment includes source code analysis, interface testing, threat modelling, and verification of key security functions such as secure boot, cryptographic services, key management, software isolation, secure storage, firmware update validation, and attestation.

Level 2 is suited to connected devices operating in semi-hostile environments, such as industrial controllers, smart home hubs, and medical systems, where resistance to software-based threats is critical.

Level 3: Protection Against Physical Attacks

PSA Certified Level 3 builds on Level 2 by extending the threat model to include physical attacks. In addition to demonstrating resistance to scalable software threats, devices must withstand advanced hardware-based techniques such as side-channel analysis, fault injection, and probing.

The evaluation is conducted by an independent security laboratory and includes thorough documentation review, source code analysis, and physical validation of tamper resistance measures. The PSA Root of Trust must securely implement core functions—secure boot, cryptographic operations, attestation, secure updates, and isolation, while ensuring that these cannot be bypassed through direct hardware manipulation.

Level 3 is tailored for high-value or safety-critical applications, such as automotive ECUs, smart meters, and medical devices, where physical access by adversaries is a realistic threat and strong hardware-based defences are essential.

Level 4: Highest Security Assurance

PSA Certified Level 4 is designed for the most security-critical applications, such as national infrastructure, defence, and aerospace. It introduces the most rigorous evaluation methods in the framework, including formal analysis, white-box testing, and methodical vulnerability assessments (e.g. AVA_VAN.4), to demonstrate resilience against highly sophisticated, state-sponsored threats.

Importantly, Level 4 is not necessarily “more robust” than Level 3; it is different in scope. Whereas Level 3 certifies an entire chip, Level 4 applies only to individual security components, such as Integrated Secure Enclaves (iSEs), Secure Elements (SEs), or PSA Root of Trust (PSA-RoT) modules. It does not certify full devices or chips but rather provides assurance for critical building blocks reused within higher-level systems. Level 4 establishes a valuable blueprint for organisations aiming to implement the highest standards of secure design at the component level.

Trust in a system must be built from the ground up. As a result, any claim of security at the software or device level is only credible if it's anchored in certified silicon. Without a trusted hardware foundation, upper-layer certifications lack meaningful assurance.

Security Requirement	PSA Certified Level 1 v3.1	EN 303 645	NIST 8425	California SB-327	PSTI	EU-CRA	RED
Authentication/ Password	√	√	√	√	√	√	√
Configuration	√	√	√	√		√	
Crypto	√	√	√	√		√	
Secure Communication	√	√	√	√		√	√
Hardening	√	√	√	√		√	√
Logging	√		√				√
Privacy	√	√	√	√		√	√
Secure Storage	√	√	√	√		√	√
Update	√	√	√	√	√	√	√

Alignment with Global Cybersecurity Regulations

The table above highlights how PSA Certified Level 1 (version 3.1) maps to the core security requirements of major regulatory frameworks, including EN 303 645, NIST 8425, California SB-327, UK PSTI, EU-CRA, and RED. This alignment helps developers prepare for evolving cybersecurity regulations and streamline compliance across global markets. Further details can be found in the PSA Certified Regulations Whitepaper[9].

Explanation of Security Categories Addressed by Level 1 Certification

The categories below provide high-level definitions of the security concepts referenced in the table. These help clarify how PSA Certified Level 1 addresses the core requirements found in global cybersecurity regulations:

Authentication / Password: Ensures only authorised software runs on uniquely identifiable devices by enforcing identity verification.

Configuration: Applies secure setup and management practices to maintain device integrity.

Crypto: Utilises strong cryptographic algorithms to protect data and assets.

Secure Communication: Protects data in transit to prevent leakage or interception in connected environments.

Hardening: Increases device resilience against software and hardware-based attacks.

[9] PSA Certified. *Certified regulations white paper – October 2024.* https://psacertified.org/app/uploads/2024/10/PSA_Certified_Regulations_Whitepaper_Oct_2024.pdf

Logging: Captures critical security events to support auditability and incident response.

Privacy: Implements safeguards to prevent unauthorised access to personal data.

Secure Storage: Protects sensitive information from tampering or exposure.

Update: Ensures firmware updates are authenticated, securely applied, and protected from rollback.

The PSA Root of Trust Architecture

PSA Certified promotes a clear model for device trust through the Root of Trust (RoT) architecture, which forms the foundation for security services across the device.

The PSA Root of Trust Components

The PSA Root of Trust consists of two integral parts:

1. Immutable Root of Trust

Implemented directly in hardware, the Immutable RoT remains fixed throughout production. It provides the foundational security elements:

- Device identity
- Boot integrity enforcement
- Authentication mechanisms

This immutable foundation ensures that even if other parts of the system are compromised, the core security properties remain intact.

2. **Updateable Root of Trust**

Built on the immutable base, the Updateable RoT includes trusted firmware responsible for delivering key security functions such as:

- Attestation
- Secure updates
- Isolation
- Lifecycle enforcement

Unlike the Immutable RoT, these components can be securely updated to fix vulnerabilities or add new capabilities.

Application Root of Trust

Above the PSA RoT sits the Application RoT, which builds on the PSA RoT to deliver service-specific security functionality. Operating within a constrained environment, it must safeguard underlying PSA RoT assets and secrets from higher-level layers.

A Comprehensive Security Architecture

Surrounding the RoTs is the broader system: external memory–flash, DDR, and peripherals–all of which must communicate securely with the trusted core. If any layer is compromised, the architecture is designed to contain the impact and enable detection.

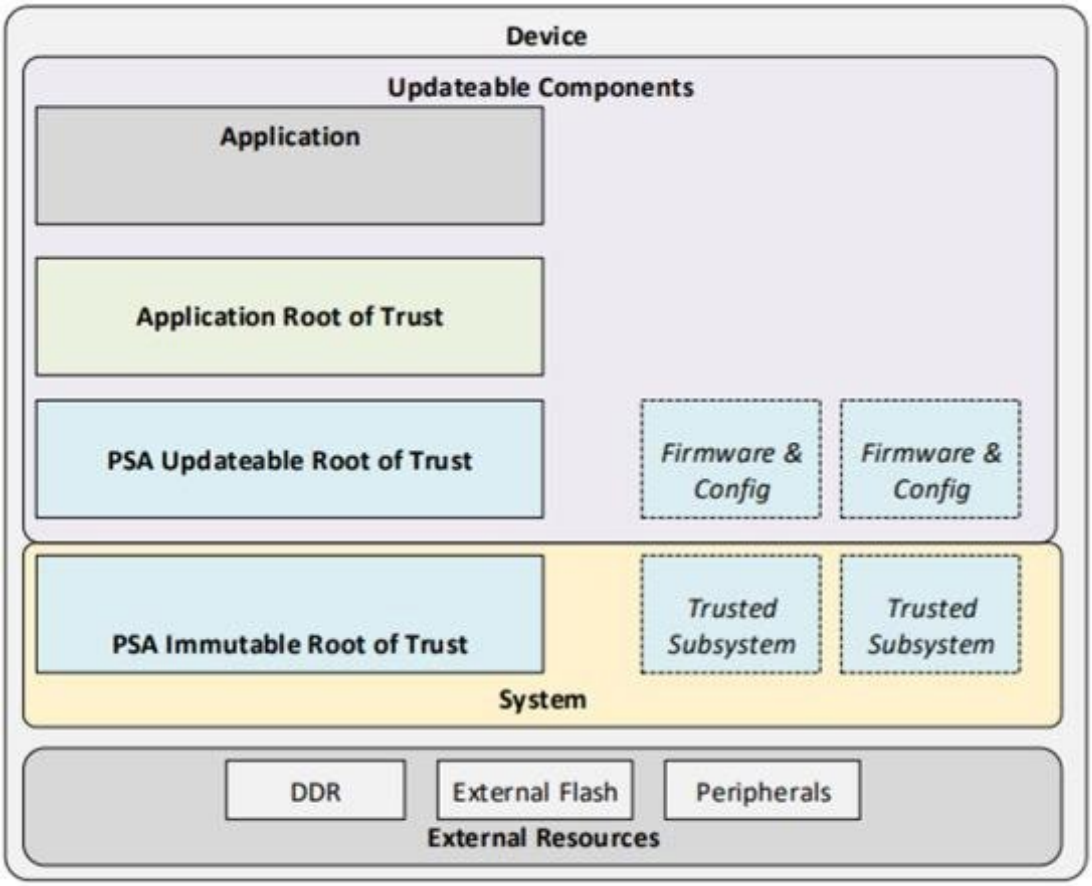
This layered design builds a chain of trust that extends from the silicon foundation to the application layer, delivering end-to-end security capable of resisting sophisticated attacks.

Architectural Implementation Considerations

Planning for PSA Certified compliance is most effective when integrated early in the architectural design phase. Attempting to retrofit a Root of Trust into an existing SoC is often inefficient and sometimes unfeasible. By incorporating secure provisioning, attestation flows, lifecycle management, and trusted key hierarchies from the outset, teams can deliver a more consistent and certifiable solution.

Security goes beyond simply selecting the right IP. Design decisions must balance trade-offs between isolation and performance, debug access and tamper resistance, or provisioning complexity and long-term support. This demands that design teams have a solid grasp of attack models, threat surfaces, and certification criteria.

For devices in industrial, automotive, healthcare, or other regulated sectors, getting these elements right is critical. Increasingly, certification is not optional—it's a prerequisite for market access.



PSA Certified device architecture showing layered Roots of Trust and trusted system components (Credit Source: Arm® Platform Security Architecture Security Model 1.0, page 18)

Implementing PSA Certified in Product Design

Security must span the full lifecycle of a device; often 10–15 years. The silicon must support secure firmware updates, key rotation, and resilience to evolving threats. That means RoTs can't just validate boot; they must support runtime enforcement, secure storage, and auditability.

Engineers need to think beyond initial certification and consider:

- How devices are provisioned during manufacturing
- How certificates are managed across product lines
- How compromise events are detected and mitigated in the field

Implementation of PSA Certified principles necessitates attention to several key areas:

Secure Provisioning and Manufacturing

A secure manufacturing process is essential for establishing device identity and initial security state. This involves:

- Secure generation and injection of unique device identifiers
- Establishment of cryptographic key material
- Programming of security lifecycle states

Lifecycle Management

Throughout a device's operational life, security must be maintained through:

- Regular security updates to address vulnerabilities
- Key rotation mechanisms to limit the impact of keys being compromised
- Secure state transitions that maintain the integrity of the security architecture

Trade-offs and Design Decisions

Implementing PSA Certified principles requires balancing competing requirements:

- **Security vs. Performance**: Strong security measures may impact system performance, requiring careful optimisation
- **Isolation vs. Resource Usage**: Robust isolation enhances security but may increase resource requirements
- **Debug Access vs. Security**: Development and testing need access that could compromise security if not carefully managed

Integration with Existing Systems

For many manufacturers, implementing PSA Certified principles means integrating secure components with existing systems. This requires:

- Careful interface design to prevent security bypasses
- Clear security boundaries between trusted and untrusted components
- Validation that the integrated system maintains security properties

PSA Certified offers a framework to structure this thinking and evaluate its implementation, helping manufacturers navigate these challenges while creating secure, certifiable products.

EnSilica's Approach to PSA Certified

At EnSilica, we use the framework defined by PSA Certification to guide our SoC customers through the cybersecurity regulation landscape, leveraging our device security experts and our in-house cryptographic accelerators.

Comprehensive Security IP Portfolio

EnSilica provides a range of security-focused IP and solutions, including our eSi-Crypto hardware cryptographic accelerators:

- **eSi-Crypto**: Our cryptographic IP library includes a wide range of encryption and authentication algorithms with low resource usage and high throughput, including:
    - Advanced Encryption Standard (AES)
    - Elliptic Curve Cryptography (ECC/ECDSA)
    - Secure Hash Algorithms (SHA1/SHA2/SHA3)
    - Post-Quantum Cryptography (PQC) including CRYSTALS Kyber and Dilithium
- **True Random Number Generators (TRNG)**: Fully compliant with NIST 800-22, our TRNG provides high-quality random numbers essential for cryptographic operations.

These hardware-based cryptographic solutions offer several advantages over software implementations:

- Higher performance with lower power consumption
- Better protection against side-channel attacks
- Reduced load on the main processor
- Greater resistance to tampering

Security-First Design Methodology

Our design methodology places security at the forefront of the development process:

1. **Early Security Requirements Analysis**: We work with customers to identify security requirements based on their specific use case, regulatory landscape, and threat model
2. **PSA-Aligned Architecture**: Our designs incorporate PSA Certified principles from the beginning, ensuring that security is built in rather than added on
3. **Secure Implementation**: Our development processes follow security best practices, with rigorous testing and validation throughout
4. **Certification Support**: We provide comprehensive support for PSA Certified evaluation and certification, helping customers navigate the certification process

Supporting the Full Security Lifecycle

Security doesn't end with product delivery. EnSilica supports customers throughout the entire security lifecycle:

1. **Secure Manufacturing**: We help establish secure provisioning processes during manufacturing
2. **Ongoing Maintenance**: Our solutions support secure updates and long-term security maintenance

3. **Regulatory Compliance**: We help customers meet evolving regulatory requirements across multiple jurisdictions
4. **Vulnerability Management**: We provide ongoing support for addressing and mitigating security vulnerabilities

As a UK-based fabless ASIC supplier working across automotive, industrial, and communications sectors, EnSilica brings deep experience in silicon design that enables customers to reduce design complexity, accelerate time to market, and confidently meet evolving security and regulatory requirements.

Conclusion: Building Trust from the Silicon Up

As the cybersecurity landscape evolves, product security can no longer be treated solely as a software or system-level concern—it must begin at the silicon. If the underlying hardware cannot be trusted, the integrity of everything built on top of it is inherently compromised.

PSA Certified offers a structured, multi-layered approach to demonstrating that a device is secure by design, aligned with global regulations, and resilient against both known and emerging threats. For engineering teams, it defines clear, actionable security objectives. For systems companies, it builds assurance throughout the supply chain.

Key takeaways from this white paper include:

1. **Security Extends Beyond Connectivity**: Any device with digital functionality requires robust protection, regardless of internet access

2. **Regulatory Pressure is Rising**: Global legislation is driving proactive, lifecycle-based security expectations

3. **Hardware is the Foundation**: True device security starts at the silicon level, with hardware designed to enforce and sustain protection

4. **PSA Certified Brings Structure**: The framework provides a clear, scalable path to implement and validate security at multiple assurance levels

5. **Certification Builds Confidence**: Independent evaluation strengthens trust with customers, partners, and regulators alike

For those developing digital products, the message is clear: trust must be built from the bottom up. By adopting PSA Certified principles and partnering with experienced design specialists like EnSilica, manufacturers can deliver devices that are secure by design, resistant to sophisticated attacks, and ready to meet the demands of a more regulated world.

In an environment where security is becoming a key differentiator, and compliance a condition of market entry, selecting the right silicon partner has never been more important.