Joint Whitepaper

Marvell Government Solutions, LLC

InfoSec Global, Inc.

Quantum-Ready Hardware and Software Platform Secured by Cryptographic Agility

July 2023

www.marvell.com

mgssales@marvellgs.com

www.isgfederal.com

info@isgfederal.com

1. Background

When the first cryptographic algorithms were standardized near the beginning of the digital age, it was believed that they would remain secure for the foreseeable future. Over the few decades, combining new cryptanalytic attacks and the continued advancement of computers has led to the depreciation of much of early cryptography. Even today, cryptographic algorithms continue to be depreciated and replaced.

Developments in quantum computing pose threats to our public-key infrastructure (PKI). In response, the National Institute of Standards and Technology (NIST) proposed to standardize new post-quantum cryptographic (PQC) algorithms that will remain resistant to any known attacks by adversaries with access to future powerful quantum computers.

Existing cryptographic solutions will urgently need major redesign efforts to support these new NIST standards. However, updating an already-deployed hardware system is expensive and resource-intensive. Software reuse is complex, and implementing new algorithms is a lengthy process. As a result, vulnerable systems are left operational in unpatched states until field repairs can be executed. A co-developed hardware and software solution is the only way to future-proof products and create an agile and secure system.

1.1. Solution Compliance

Managing security in complex chiplet-based systems requires increased diligence in the design, verification, deployment, and lifecycle management phases. The capability to migrate quickly and seamlessly to PQC is essential for next-generation systems. New chips and systems should be designed with built-in crypto-agility as a foundational element. Software must support and comply with new PQC standards that can be deployed securely and rapidly across devices and ecosystems of devices through one common platform. Security must be included across the system's lifecycle, ensuring that attacks are thwarted and crypto compliance is ensured as new standards are rolled out or vulnerabilities identified.

1.2. How Marvell Government Solutions and InfoSec Global's Agile Secure Chiplet addresses real-world cryptography compliance

Marvell Government Solutions (MGS), a subsidiary of Marvell Semiconductor, and InfoSec Global (ISG) have partnered to develop a next-generation hardware and software platform for future-proof, secure, and agile cryptography. MGS has security capabilities that span multiple levels of hardware designs – from IP building blocks such as embedded Hardware Security Modules (eHSM) and IPsec & MACsec for custom ASICs, to standard product chips and boards that address security concerns over many hardware domains. As a fabless provider, Marvell has deep supply partnerships at commercial scale across several fabricators and OSATs. MGS also has over 15 years of experience in Secure Design and Testing.

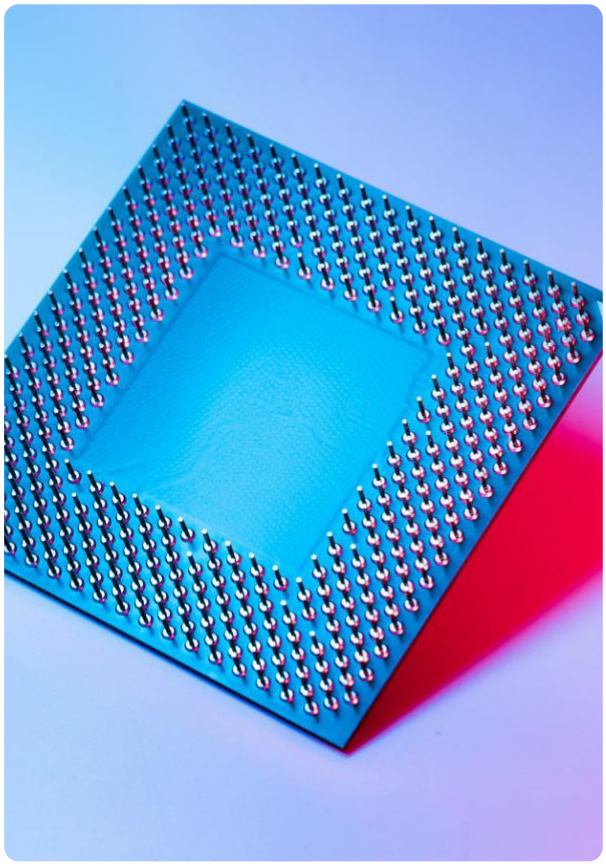
ISG provides next-generation cryptographic discovery, agility, and management solutions from the silicon firmware up through end-point applications. InfoSec Global's secure software enables the management and agility of all cryptographic assets across a digital ecosystem, resulting in the ability to automate and orchestrate cryptographic migrations across networks of connected assets.

Our Agile Secure Chiplet – built on post-quantum-ready eHSM and an Agile software stack – allows customers to migrate their systems to the latest cybersecurity algorithms, to manage assets in the field, and ensure compliance with ever-changing standards. These combined hardware and software components are designed together from the ground up, ensuring next-generation security solutions that are programmable, upgradeable, expandable, and secure.

The Agile eHSM Platform employs leading-edge hardware technology to achieve performance targets, with a trusted and future-proof software platform to upgrade the installed hardware base against new emergent security threats. Architecting security from Marvell Hardware Security Module (HSM) and the InfoSec Global Software Development Kit (SDK) will build crypto-agility into the interface allowing for easy migration to PQC algorithms and simpler certification of solutions.

2. Hardware

Marvell has extensive SoC development experience, including security and anti-tamper technologies. Our Hardware Security Module experience builds on multiple generations of security chips going back to 2012 and has been used in cellphone, WAN, storage, automotive and network infrastructure environments. MGS is proposing a security chiplet based on silicon-proven IP. The IP is FIPS140-3 certified.



2.1. Agile Secure Chiplet

The Agile Secure Chiplet is a complete System-on-Chip solution for security in advanced packaging systems. It ensures platform security with Marvell's state-of-the-art Hardware Security Module (HSM), which includes a hardware-based Root of Trust to implement secure boot and encrypted boot that protects against equipment theft, unauthorized access to sensitive data, unauthorized hardware component replacement, eavesdropping or data injection.

It also monitors for side channel attacks and is designed to provide security to devices downstream by managing keys and authenticating the system upon boot and only allowing data traffic once the system is deemed secure. Downstream devices can be other chiplets, ASICs, FPGAs (including personalization data), or standard products. These devices can be on-module or off-module.

2.2. eHSMPQ™

At the root of the agile hardware solutions is the Marvell eHSMPQ™. This IP provides FIPS 140-3 certified trusted services to the security chiplet. It supports Life Cycle Management, Secure Boot, Encrypted Boot, and Measured Boot Root of Trust Services.

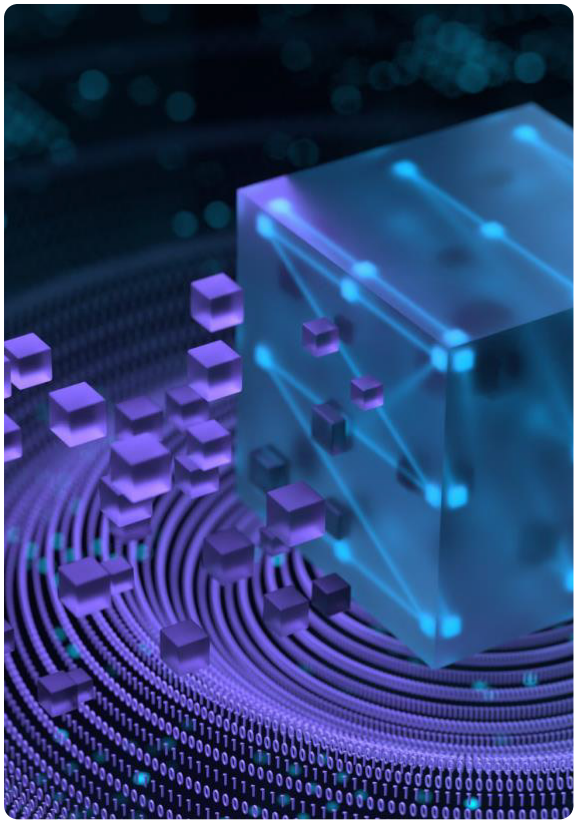
It has side-channel protection sensors to monitor side-channel attacks, providing an exception signal to the device if an attack is detected. The eHSMPQ™ uses a hardware-based Root of Trust for measurement, reporting and identification. This ensures a hardware-rooted secure storage of keys and a hardware-rooted chain of trust for authentication.

Most contemporary digital security relies on a combination of both public-key and symmetric cryptography. To resist attacks from any quantum computer, symmetric cryptography must be updated to have large enough key sizes, while public-key cryptography must be replaced entirely by new quantum-resistant algorithms – for example, NIST's public-key PQC algorithms.

The eHSMPQ™ crypto Engine pool supports symmetric and public key encryption schemes. The symmetric engines support sufficient length keys to be PQ resilient. The public key engines support PQC schemes that have been selected for NIST standardization such as CRYSTALS-KYBER, CRYSTALS-Dilithium, SPHINCS+ and Falcon, as well as the standardized stateful hash-based algorithms LMS and XMSS.

2.3. Hardware Summary

The eHSM is the gatekeeper for the chiplet based system. All chiplets in a system must be authenticated and trusted before they can be used. The eHSM manages the links to and from other chiplets using Pre Shared Keys (PSK).



It only enables data traffic to other chiplets via standards such as IDE in PCIe port and MACsec in the Ethernet subsystem. Encrypted data flows to downstream chiplets only after secure boot, system chiplet authentication and port authentication. In this manner, the system is secure. The eHSM will recognize if unauthorized devices have been introduced and deny access to compromised components.

Marvell is participating in industry forums that are developing secure interface solutions for chiplet based systems. The interfaces and inter-chiplet security protocols are evolving to ensure that on-module communications are secured and attack resilient, irrespective of supplier and chiplet content. Until all chiplets comply with future accepted standards, security design reviews will be required to address security of chiplets that might not have Root-of-Trust IP.

3. Software

3.1. Introduction

Next-generation chips and chiplets will need to be robust, agile and afford higher levels of overall functionality. In response and in direct partnership with MGS, ISG proposes an eHSM device incorporating the InfoSec Global SDK, cryptographic agility API ecosystem, and Trust Authority (TA) framework. This combination will provide maximum flexibility for diverse eHSM use-cases and paves the way for next-generation PQC compatibility. ISG commits to develop an ecosystem of open APIs for hardware devices to prevent vendor lock while maximizing interoperability for future migration to different design packages. The ISG software is backed by a team of world-leading cryptographic experts who have direct involvement with current and future cryptographic standards development, covering classical and post-quantum primitives.

Today there are major obstacles to PQC migration:

- Software re-use is almost impossible for PQC migration
- Product certification is costly, time-consuming and complicated
- System integration, maintenance and expandability are complex

ISG's new solution puts cryptographic agility into action:

While most technology becomes outdated and needs to be replaced, cryptography is generally deprecated due to vulnerabilities. This has historically been a problem, especially since migrating cryptography is often a lengthy process.

3.2. Trust Authority

With a new focus on general-purpose applications of next-generation chiplet devices, there is a need for OEMs to provide a solution that uniquely customizes and tracks each device in the field. ISG's Trust Authority service (TA) provides this capability without compromising performance or increasing SWAP-C (Figure 1).

The TA is made possible by implementing the following elements:

- A 256b unique key is generated randomly within FIPS 140-2 level-3 boundary and personalized into eHSM
- This unique key serves as an identity for the chiplet in the future
- The mapping of these IDs with devices is stored in the appropriate IL-Level DoD cloud
- Mapping services are thereafter provided by the Trust Authority service

The TA service can be delivered as a cloud-hosted multi-tenant SaaS, or supporting on-premise deployments for higher security use-cases.

The secure management of cryptographic assets within the eHSM follows the Global Platform Trusted Execution Environment (TEE) Management Framework (TMF). Global Platform is expected to release a quantum-secure version of these standards by mid-2023. The Trust Authority will be aligned with the new quantum-secure standards once available.

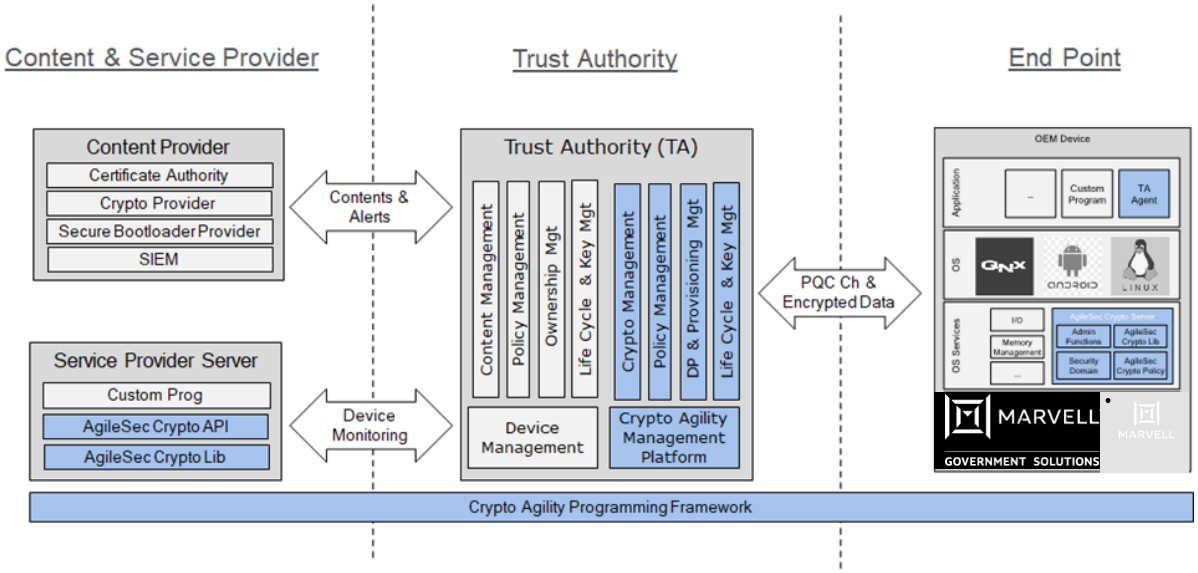


Figure 1: Crypto-Agility Ecosystem

3.3. Future Proofing PQC

ISG will provide the post-quantum algorithms as part of the embedded eHSM. The eHSM crypto server will support respective public key provisioning to the eHSM OTP bank. These algorithms include NIST standardized PQC algorithm, NIST PQC algorithms that are selected for standardization and algorithms that NIST specifies as new PQC standards continue to be released.

ISG's crypto agile SDK also includes the cryptographic algorithms that NSA has recommended for interim, as well as long-term solutions to the quantum threat, such as Kyber and Dilithium. The product's agility supports the migration to subsequent algorithms, including future standards for PQC algorithms.

4. Supply Chain Security

4.1. ISG Hardware

Enabled by leading-edge Marvell secure hardware IP, ISG's SDK can provide supplier information embedded in the hardware to track its fabrication point of origin. This allows an operator to confirm the device was sourced (designed and manufactured) by approved partners and manufactured in approved factories to help meet hardware sovereignty requirements. All the aforementioned information would be cryptographically bound with the device in support of supply-chain security objectives.

4.2. MGS Supply Chain Management

Marvell Government Solutions (MGS), a subsidiary of Marvell Semiconductor, and InfoSec Global (ISG) have partnered to develop a next-generation hardware and software platform for future-proof, secure, and agile cryptography.

MGS has over 25 years of end-to-end supply chain management – initial design, prototyping, production fulfillment and end-of-life. In conjunction with their security partner, MGS has operated a Secure Design and Test Center that includes equipment for secure wafer test, module test, and assembly. Each ASIC design has a unique identification based on Root of Trust. By maintaining secure ownership of the customer's design data, and with their secure wafer and module test environments, MGS can discover design intrusion attempts by monitoring yield and speed discrepancies versus target. Furthermore, MGS has purview over the entire chip provenance. By their nature, ASICs have unique component identities that enable traceability, including packaging. With secure supply chain monitoring, MGS works with fabs and OSATs to obtain component data at each stage to track sources of potential issues. As a result, MGS can operate a fab-agnostic hybrid supply chain flow where parts can be manufactured in any fab while maintaining the designed-in security and integrity of the supply chain.

5. Conclusion

The joint MGS / ISG Agile eHSM solution provides maximum flexibility across a traditionally rigid cryptographic ecosystem. The MGS / ISG partnership is well-positioned to identify unique and secure innovations in each area and beyond, tailored to their customer's specificity of use. With efforts underway to further introduce agility within the eHSM architecture, our team is ready to design, build and scale to the demands of next-generation cryptography.

Although challenging, the goals and vision outlined in this white paper are achievable with the right technology partners and associated intellectual talent. Such a pairing exists within the MGS and ISG partnership. Through our collective intellectual property and deep knowledge of SOTA hardware and software designs, we will provide reliable access to leading-edge chiplet packages, agile cryptographic applications, and a trusted production line supporting a more efficient and secure technology supply chain.

Marvel press releases on eHSM:

- Marvell Launches LiquidSecurity 2 Module to Empower Best-in-Class Hardware HSM-as-a-Service for the Multi-Cloud Era

  https://www.marvell.com/company/newsroom/marvell-liquidSecurity2-hardware-security-multi-cloud-era.html

- Introducing Marvell's Third Generation Brightlane™ Ethernet Switch

  https://www.marvell.com/content/dam/marvell/en/company/media-kit/automotive/marvell-brightline-ethernet-switch-media-presentation.pdf