WHITE PAPER

Earning Digital Trust

Intrinsic ID QuiddiKey 300: The First Root-of-Trust IP PSA Certified Against Physical Attacks

psacertified™

level three RoT component

INTRINSIC ID®

Executive Summary

The rapid growth of the internet of things (IoT) has caused a parallel concern for the security of billions of connected devices. Any unprotected device could become the entry point for an attack on the device itself, or the networks on which it runs. To secure the IoT, each piece of silicon in the supply chain needs to be trusted. The best way to achieve this is by using a hardware-based root of trust (RoT) for every device. This is a seemingly unachievable goal; however, collaboration among industry players on standards and certifications can make it more attainable. The PSA Certified 2023 Security Report indicates that 72% of tech decision makers are interested in the development of an industry-led set of guidelines to make reaching the goal of a secure IoT more attainable. One important industry-led effort in standardizing IoT security that has been widely adopted is PSA Certified. PSA stands for Platform Security Architecture and PSA Certified is a global partnership addressing security challenges and uniting the technology ecosystem under a common security baseline, providing an easy-to consume and comprehensive methodology for the lab-validated assurance of device security. Intrinsic ID QuiddiKey, which has been deployed in over 500 million chips, is the first-ever IP solution to be awarded “PSA Certified Level 3 RoT Component.” This certifies that the IP includes substantial protection against both hardware and software attacks.

The IoT is Growing Fast and So Are Security Concerns

The internet of things (IoT) has been growing at a fast pace. As of 2023, there are now double the number of internet connected devices – 16 billion – than people on the planet. However, many of these devices are not properly secured. The high volume of insecure devices being deployed is presenting hackers with more opportunities than ever before: on average there are 5,400 attacks per month on IoT devices, with 7 million data records compromised daily. Governments around the world are realizing that additional security standards for IoT devices are needed to address the growing and important role of the billions of connected devices we rely on every day. The EU Cyber Resilience Act, and the IoT Cybersecurity Improvement Act in the United States are driving improved security practices as well as an increased sense of urgency.

Digital trust is critical for the continued success of the IoT. This means that security, privacy, and reliability are becoming top concerns. IoT devices are always connected and can be deployed in any environment, which means that they can be attacked via the internet as well as physically in the field. Whether it is a remote attacker getting access to a baby monitor or camera inside your house, or someone physically tampering with sensors that are part of a critical infrastructure, IoT devices need to have proper security in place.

This is even more salient when one considers that each IoT device is part of a multi-party supply chain and is used in systems that contain many other devices. All these devices need to be trusted and communicate in a secure way to maintain the privacy of their data. It is critical to ensure that there are no backdoors left open by any link in the supply chain, or when devices are updated in the field. Any weak link exposes more than just the device in question to security breaches; it exposes its entire system – and the IoT itself – to attacks.

A Foundation of Trust Starts in the Hardware

To secure the IoT, each piece of silicon in the supply chain needs to be trusted. The best way to achieve this is by using a hardware-based root of trust (RoT) for every device. An RoT is typically defined as "the set of implicitly trusted functions that the rest of the system or device can use to ensure security." The core of an RoT consists of an identity and cryptographic keys rooted in the hardware of a device. This establishes a unique, immutable, and unclonable identity to authenticate a device in the IoT network. It establishes the anchor point for the chain of trust, and powers critical system security use cases over the entire lifecycle of a device.

Protecting every device on the IoT with a hardware-based RoT can appear to be an unreachable goal. There are so many types of systems and devices and so many different semiconductor and device manufacturers, each with their own complex supply chain. Many of these chips and devices are high-volume/low-cost and therefore have strict constraints on additional manufacturing or supply chain costs for security. The PSA Certified 2023 Security Report recently indicates that 72% of tech decision makers are interested in the development of an industry-led set of guidelines to make reaching the goal of a secure IoT more attainable.

Security Frameworks and Certifications Speed-Up the Process and Build Confidence

One important industry-led effort in standardizing IoT security that has been widely adopted is PSA Certified. PSA stands for Platform Security Architecture and PSA Certified is a global partnership addressing security challenges and uniting the technology ecosystem under a common security baseline, providing an easy-to-consume and comprehensive methodology for the lab-validated assurance of device security. PSA Certified has been adopted by the full supply chain from silicon providers, software vendors, original equipment manufacturers (OEMs), IP providers, governments, content service providers (CSPs), insurance vendors and other third-party schemes. PSA Certified was the winner of the IoT Global Awards "Ecosystem of the year" in 2021.

PSA Certified lab-based evaluations (PSA Certified Level 2 and above) have a choice of evaluation methodologies, including the rigorous SESIP-based methodology (Security Evaluation Standard for IoT Platforms from GlobalPlatform), an optimized security evaluation methodology, designed for connected devices. PSA Certified recognizes that a myriad of different regulations and certification frameworks create an added layer of complexity for the silicon providers, OEMs, software vendors, developers, and service providers tasked with demonstrating the security capability of their products. The goal of the program is to provide a flexible and efficient security evaluation method needed to address the unique complexities and challenges of the evolving digital ecosystem and to drive consistency across device certification schemes to bring greater trust.

The PSA Certified framework recognizes the importance of a hardware RoT for every connected device. It currently provides incremental levels of certified assurance, ranging from a baseline Level 1 (application of best-practice security principles) to a more advanced Level 3 (validated protection against substantial hardware and software attacks).

PSA Certified RoT Component

Among the certifications available, PSA Certified offers a PSA Certified RoT Component certification program, which targets separate RoT IP components, such as physical unclonable function or PUF subsystems, which use unclonable properties of silicon to create a robust trust (or security) anchor. As shown in Figure 1, the PSA-RoT Certification includes three levels of security testing. These component-level certifications from PSA Certified validate specific security functional requirements (SFRs) provided by an RoT component and enable their reuse in a fast-track evaluation of a system integration using this component.

Device

- Consumes silicon and system software certification
- Built on PSA-RoT
- Aligns with standards / regulations
- Ready for further certifications

System Software
(RTOS and Linux Applications)

- Leverages PSA Root of Trust security functions
- Eligible for PSA Certified Level 1
- Evaluates security best practice

Silicon

- Implements PSA-RoT
- Evaluated with three levels of security robustness testing including best practice, software attacks and hardware attacks

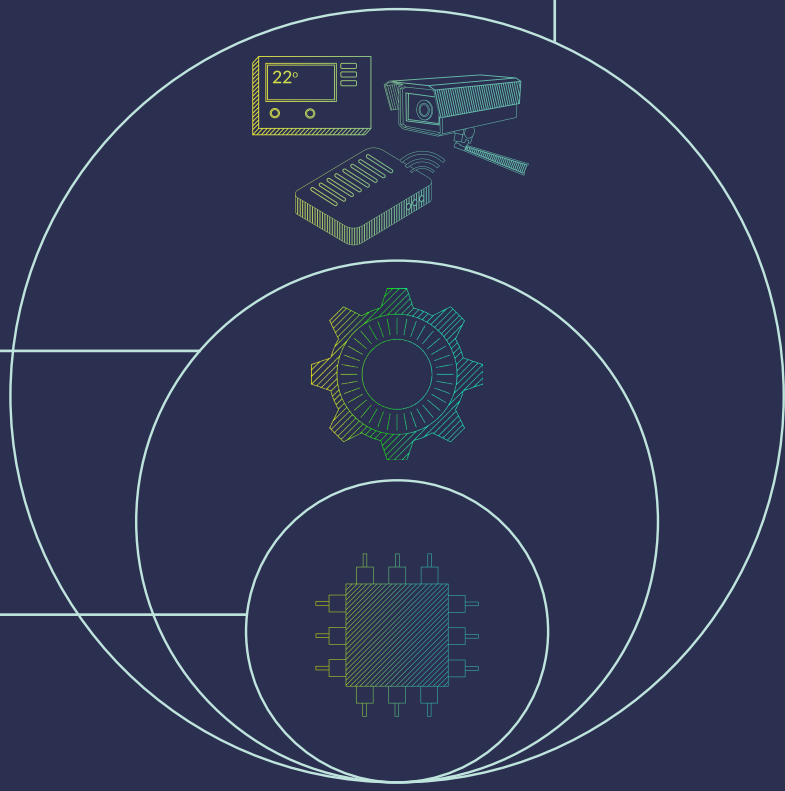


Figure 1. PSA Certified establishes a chain of trust that begins with a PSA-RoT

Intrinsic ID QuiddiKey, a Proven RoT IP Solution, Now PSA Certified

Intrinsic ID QuiddiKey® hardware IP is a secure key generation and storage solution that enables device manufacturers and designers to secure their products with internally generated unclonable identities and device-unique cryptographic keys. It uses the inherently random start-up values of SRAM as a physical unclonable function (PUF), which generates the entropy required for a strong hardware root of trust.

This root key created by QuiddiKey from the PUF is never stored, but rather recreated from the PUF upon each use, so there is never a key to be discovered by attackers. The root key is the basis for key management capabilities that enable each member of the supply chain to create its own secret keys, bound to the specific device, to protect their IP/communications without revealing these keys to any other member of the supply chain.

QuiddiKey offers robust PUF-based physical security, with the following properties:

- No secrets/keys at rest (no secrets stored in any memory)
  - prevents any attack on an unpowered device
  - keys are only present when used, limiting the window of opportunity for attacks
- Hardware entropy source/root of trust
  - no dependence on third parties (no key injection from outside)
  - no dependence on security of external components or other internal modules
  - no dependence on software-based security
- Technology-independent, fully digital standard-logic CMOS IP
  - all fabs and technology nodes
  - small footprint
  - re-use in new platforms/deployments
- Built-in error resilience due to advanced error-correction

The Intrinsic ID PUF technology has been field-proven over more than a decade of deployment on over 500 million chips. And now, the Intrinsic ID hardware solution QuiddiKey 300 has achieved a new milestone by becoming the world's first IP solution to be awarded "PSA Certified Level 3 RoT Component." This certifies that the IP includes substantial protection against both software and hardware attacks (including side-channel and fault injection attacks) and is qualified as a trusted component in a system that requires PSA Level 3 certification.

Fault Detection and Other Countermeasures

In addition to its PUF-related protection against physical attacks, all QuiddiKey products have several built-in physical countermeasures. These include both systemic security features (such as data format validation, data authentication, key use restrictions, built in self-tests (BIST), and heath checks) as well as more specific countermeasures (such as data masking and dummy cycles) that protect against specific attacks.

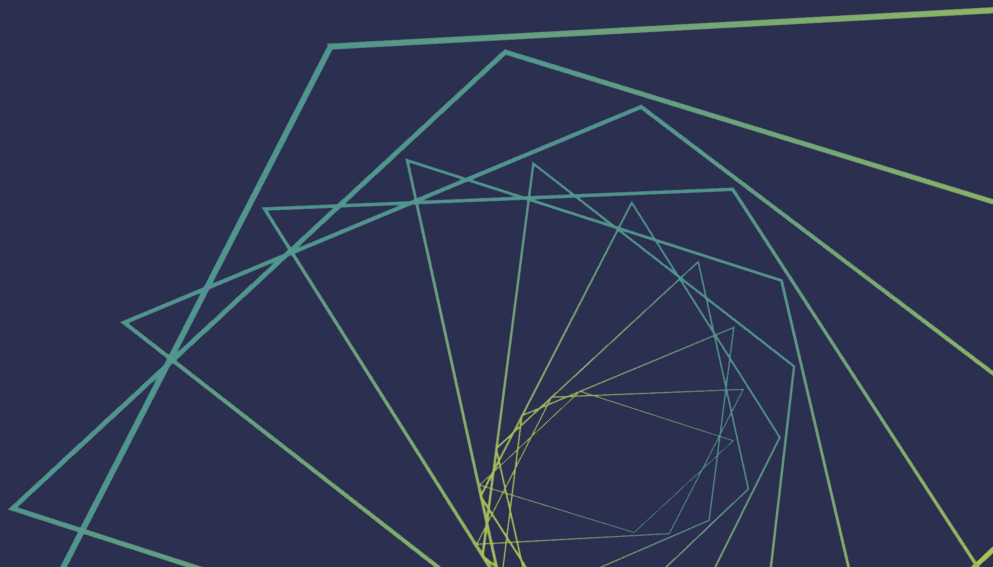
QuiddiKey 300 goes even one step further. It is a version of QuiddiKey that validates all inputs through integrity checks and error detection. It continuously asserts that everything runs as intended, flags any observed faults, and ensures security. Additionally, QuiddiKey 300 provides hardware and software handholds to the user which assist in checking that all data is correctly transferred into and out of QuiddiKey. The QuiddiKey driver also supports fault detection and reporting.

Advantages of PUFs over Key Injection and OTP storage

For end-product developers, a PUF solution like QuiddiKey 300 has many advantages over traditional approaches for key management. These traditional approaches typically require key injection (provisioning secret keys into a device) and some form of non-volatile memory (NVM), such as embedded Flash memory or one-time programmable storage (OTP), where the programmed key is stored and where it needs to be protected from being extracted, overwritten, or changed. Unlike these traditional key injection solutions, QuiddiKey does not require sensitive key handling by third parties, since PUF-based keys are created within the device itself. In addition, QuiddiKey offers more flexibility than traditional solutions, as keys protected by the PUF can be added at any time in the lifecycle rather than only during manufacturing.

In terms of key storage, QuiddiKey offers higher protection against physical attacks than storing keys in some form of NVM. PUF-based root keys are not stored on the device, but they are reconstructed upon each use, so there is nothing for attackers to find on the chip. Instead of storing keys in NVM, QuiddiKey stores only (non-sensitive) helper data and encrypted keys in NVM. The traditional approach of storing keys on the device in NVM is more vulnerable to physical attacks.

Finally, QuiddiKey provides a lower-cost solution, as it can protect a virtually unlimited number of encrypted keys in inexpensive NVM on- or off-chip. Traditional key storage often requires expensive physical protection for the memory in which the root key is stored. Furthermore, protected NVM and OTP storage is very challenging and expensive to manufacture reliably in advanced CMOS technology nodes. QuiddiKey offers a process-independent solution for key storage, as it is based on the properties of basic process elements (SRAM) rather than specialized storage.



PSA Certified Level 3 Evaluation of QuiddiKey 300

Independent test labs are used for PSA RoT evaluations, creating consistency and standardization and third-party validation of security implementations. This ensures that all IoT components and products are built to a consistent set of security principles. Finally, a certificate is issued by an independent certification body based on an objective assessment of the evaluation lab's findings.

To achieve PSA Certified Level 3 RoT Component certification, an RoT component must provide evidence of protection against hardware and software attacks. This requires a lab-based vulnerability analysis and penetration testing of the PSA-RoT security component. Two evaluation methodologies can be employed: the PSA Certified Level 3 PSA-RoT Protection Profile (informal CSPN style) or the PSA Certified Level 3 GlobalPlatform SESIP Profile (formal style).

During the 35 day-duration of the evaluation period, the RoT component must demonstrate substantial security assurance and robustness and provide evidence of protection from hardware and software attacks. This includes a security target review, a white-box vulnerability assessment and a penetration testing phase.

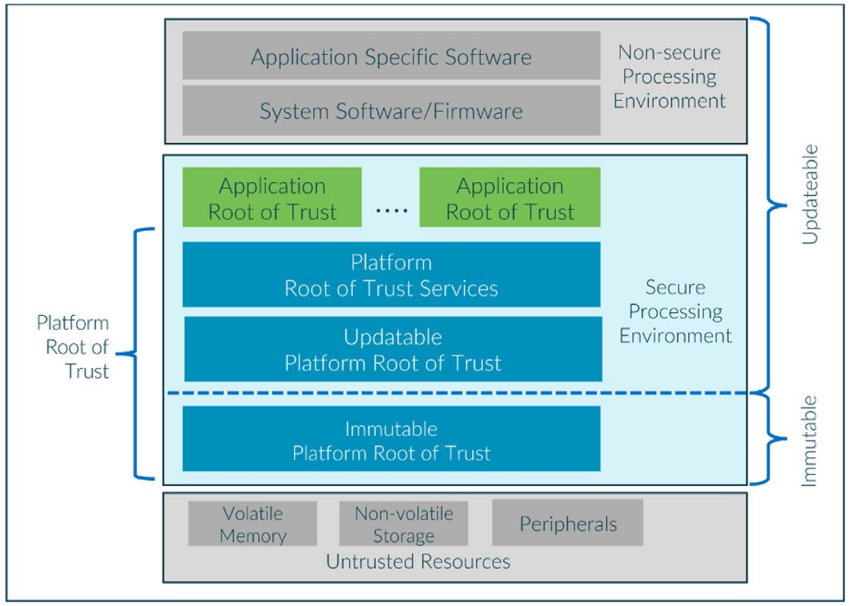


Figure 2: The (minimal) platform security model as put forward by PSA Certified (source)

Figure 2 schematically shows the platform security model as assumed by PSA Certified. As a hardware IP module, QuiddiKey and the SRAM PUF attached to it will be part of the Immutable Platform Root of Trust subsystem in this model. The security system which integrates QuiddiKey and interfaces with it, e.g., through the QuiddiKey driver library, is also assumed to reside in the Platform Root of Trust, possibly at a higher layer. The scope of the evaluation of QuiddiKey as a PSA Certified RoT Component is focused on its integration as an immutable RoT component in hardware.

As a RoT component in the PSA Certified ecosystem, QuiddiKey fulfills a number of well-defined security functional requirements (SFRs) which the integrating system can automatically inherit as part of its own certification process. Since QuiddiKey is evaluated under the formal SESIP protection profile, the claimed SFRs come from that profile. The specific SFRs for which QuiddiKey is evaluated and certified are:

- Verification of Platform Identity
- Verification of Platform Instance Identity
- Cryptographic Operation
- Cryptographic Random Number Generation
- Cryptographic Key Generation
- Cryptographic Key Storage
- Physical Attacker Resistance

Conclusion

The large and steady increase in devices connected to the IoT also increases the need for digital trust and privacy. This requires flexible and efficient IoT security solutions that are standardized to streamline implementation and certification across the multiple players involved in the creation and deployment of IoT devices. The PSA Certified framework offers an easy-to-consume and comprehensive methodology for the lab-validated assurance of device security.

Intrinsic ID QuiddiKey, which has been deployed in over 500 million chips, is the first-ever IP solution to be awarded “PSA Certified Level 3 RoT Component.” This certifies that the IP includes substantial protection against hardware and software attacks. QuiddiKey offers IoT device makers a robust PUF-based security anchor with trusted industry-standard certification and offers the perfect balance between strong security, high flexibility, and low cost.