Product Brief

Intel® Assured Supply Chain

Background

The integrity of the semiconductor supply chain is paramount in today's competitive market, but the risks from counterfeit components are significant[1], and users who rely on chips to power data centers, servers, and PCs face challenges in confirming the provenance of their processors. In addition, numerous frameworks exist to enhance supply chain security that support the public and private sectors.

To address these concerns, Intel Products created Intel® Assured Supply Chain (Intel® ASC) —a modern solution designed to provide additional transparency and assurance in the silicon manufacturing process. This specialized client System on Chip (SoC) solution provides a digitally attestable chain of custody of each chip's progress through the chip manufacturing process, leveraging a dedicated chip manufacturing pathway through specific Intel manufacturing locations. This brief describes the Intel® ASC, highlighting its strategic advantages, manufacturing process, and the timeline for product launch.

Problem Statement

Ensuring the integrity of hardware is critical to avoid financial losses, reputational damage, system downtime, and delayed recovery.

PC component supply chain transparency is a top priority for IT, with the PC representing the largest attack surface in the digital ecosystem. A growing number of attacks target layers below the OS, such as firmware and hardware components. Since 2018, the National Institute of Standards and Technology (NIST) has reported a 500% increase in firmware attacks[2].

To enhance supply chain transparency, Intel Products has developed Intel® ASC.

Intel's Strategic Advantage in Supply Chain Risk Management

Intel is uniquely positioned to address supply chain risk due to its diverse geographic manufacturing capabilities, leading ecosystem position, and#1 Rated Product Security Assurance[3]. With a robust network of manufacturing facilities in locations around the globe and strong ecosystem partnerships, Intel can offer an enhanced and verifiable mechanism for securely storing and verifying various locations and steps in a chip's manufacturing, allowing for additional transparency in the silicon manufacturing process.

Product Definition

1) **Pre-Determined Manufacturing Corridor:** The Intel® ASC manufacturing process follows a predetermined corridor. Intel® ASC encompasses every step in the silicon manufacturing process, including fabrication, die prep and sort, assembly, test, manufacturing, and warehousing. Silicon products manufactured as part of Intel® ASC deliver an end-to-end manufacturing process isolated to only the pre-determined flow. This manufacturing process offers added transparency in the overall PC system build.

2) **Secure Digital Attestation:** Customers will be able to attest to the processor being Intel® ASC from the processors brand string. Intel® ASC products will have the letter "A" at the end of the processor brand string. Using industry tools, end customers will be able to display the list of countries for the Intel® ASC SKU and verify the product's chain of custody through each step in the manufacturing process. This ability to digitally attest to the locations of silicon manufacturing provide enhanced silicon supply chain transparency.

Addressing Supply Chain Security Frameworks

The Intel Assured Supply Chain aligns to various US and European government frameworks including but limited to:

DFARS 246.870-2 - The Defense Federal Acquisition Regulation Supplement (DFARS) 246.870-2 addresses the identification and prevention of counterfeit electronic components in contractors' supply chains.

NIST SP800-161 r1 - The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161 r1 provides guidance on identifying, assessing, and mitigating cybersecurity risks throughout supply chains.

Trusted Computing Group Platform Certificate Specification v1.1 - The Trusted Computing Group (TCG) Platform Certificate Specification v1.1 outlines standards for platform certificates used in trusted computing environments.

NIST NCCOE SP1800-34 (A, B, C) - The NIST National Cybersecurity Center of Excellence (NCCOE) SP1800-34 (A, B, C) validates the integrity of computing devices and provides guidance on cybersecurity practices related to supply chain risk management.

US Government CHIPs Act - The US Government CHIPs Act mandates the creation of a strategy to identify and address potential security risks in the semiconductor supply chain. This includes issues related to access, availability, confidentiality, integrity, and geographic diversification.

European Union Directive (EU) 2022/2555 (NIS2) - The directive mandates that each Member State adopt a national cybersecurity strategy, which includes policies for supply chain security, vulnerability management, and cybersecurity education and awareness.

Products and Timelines

Initial rollout of Intel® ASC is available on select Intel® Core Ultra Series 2 commercial mobile and desktop SKUs with production and first customer ship scheduled for the third quarter of 2025. Intel is working with our OEM partners to identify a product portfolio to meet end customers' needs in large enterprises, highly regulated industries, and government segments.   Customer feedback, market analysis, and time of manufacturing will drive future location decisions and product offerings.

Intel's Commitment to Supply Chain Resilience

Intel's commitment to a resilient supply chain has never been stronger with Intel® ASC as the newest evolution in product confidence. In addition to Intel® Tiber™ Transparent Supply Chain, which enables customers the ability to better identify counterfeit or dubious platform hardware and firmware components, Intel® ASC provides an additional level of confidence by enabling a digitally attestable, and pre-determined silicon manufacturing corridor. Collectively, these unique Intel solutions help end customers mitigate risks, support industry-standard supply chain security frameworks, and provide enhanced product manufacturing transparency. Click here to learn more about Intel® Tiber™ Transparent Supply Chain

Conclusion

The need for robust and resilient silicon supply chain solutions has never been greater. With its unique position in the industry and global manufacturing footprint, Intel is well-equipped to deliver a predetermined silicon manufacturing flow and offer enhanced supply chain transparency. Intel has a long-standing reputation for delivering products built with supply chain resilience in mind, making Intel the ideal silicon partner to deliver this solution to the market.

Click here to learn more about Intel® Assured Supply Chain

1. SMT Corp., "The Growing Threat of Counterfeit Electronic Parts in the Critical Infrastructure Supply Chain of the United States and Allies", November 9, 2023. https://smtcorp.com/counterfeit-electronic-components/
2. Microsoft Security Team, "New Security Signals study shows firmware attacks on the rise; here's how Microsoft is working to help eliminate this entire class of

threats", March 30, 2021. https://www.microsoft.com/en-us/security/blog/2021/03/30/new-security-signals-study-shows-firmware-attacks-on-the-rise-heres-how-microsoft-is-working-to-help-eliminate-this-entire-class-of-threats/#:~:text=Firmware%20provides%20fertile%20ground%20to,a%20security%20threat%20versus%20firmware

3. Intel, 2024 Intel® Product Security Report, February 3, 2025. https://www.intel.com/content/www/us/en/content-details/846149/2024-intel-product-security-report.html?DocID=846149

Notices & Disclaimers

Intel technologies may require enabled hardware, software, or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.