Product Brief

Independent Attestation by Intel® Trust Authority

Put Zero Trust Within Reach and Get Public Cloud Flexibility with Private Cloud Security

Data is one of your most valuable assets. You should be able to trust the systems that run it.

When datasets contain sensitive information or intellectual property, or are subject to heightened compliance, enterprise organizations may require confidential computing workloads and environments to be verified by a third party that is operationally independent from the infrastructure provider. To solve this requirement, Intel is introducing a zero-trust, SaaS approach to attestation, rooted in silicon and scalable across multiple workloads and cloud environments—regardless of who provides the infrastructure.

Introducing a Consistent, Independent, Scalable Attestation Service

Intel Trust Authority is a new portfolio of software and services that brings enhanced security and assurance to Confidential Computing with Zero Trust principles. In its first generation, Intel Trust Authority offers an independent attestation service that attests to Trusted Execution Environments (TEEs) that are based on Intel® Software Guard Extensions (Intel® SGX) and Intel® Trust Domain Extensions (Intel® TDX). This single, consistent attestation process provides assurance to any relying party that the TEE and any data and workloads within it have not been compromised.

Intel Trust Authority's attestation service operates independently of the cloud or edge infrastructure provider that hosts your confidential computing workloads. It's cloud-agnostic and designed to work across on-premises, hybrid, and multi-cloud environments. You can configure and maintain security policies consistently across cloud deployments without having to build and maintain an expensive and complex attestation service.

Implement the tenets of Zero Trust without incurring the cost and complexity of building your own attestation service.

Independent

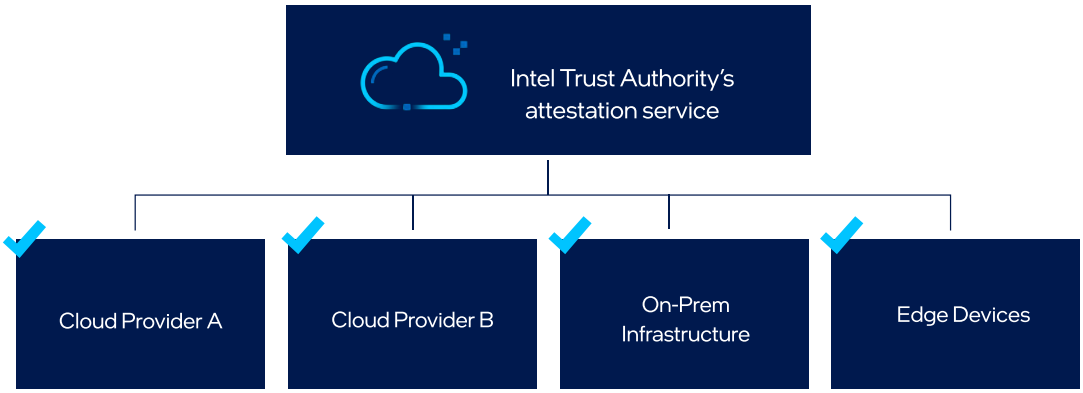
Intel Trust Authority's attestation service independently verifies the trustworthiness of the confidential computing TEE, regardless of who manages the data center. This approach addresses increasing demand for separation of duties between cloud provider and the source of attestation.

Scalable

Because Intel Trust Authority's attestation service is cloud-agnostic, organizations can deploy it to scale their confidential computing environment while maintaining a single independent attestation service and consistent security policies.

Easy to Deploy

Built as a SaaS, Intel Trust Authority's attestation service is straightforward to deploy and use. Dynamically configure security policies and retain consistency across edge, hybrid, and cloud deployments.



How It Works

Intel Trust Authority's attestation service validates cryptographically signed evidence from the TEE against customer configured policies of expected identity and integrity measurements. The SaaS then generates proof of verification in the form of an attestation token that it cryptographically signs if attestation is successful. The attestation token can be verified by any relying party. The workload verifies the signature of the token to ensure that it is a genuine Intel Trust Authority's attestation token. If so, the claims in the token are verified and the workload can be decrypted and run within the TEE.

Independent Attestation by Intel® Trust Authority

1. Set up or request from your cloud infrastructure provider a confidential computing environment (TEE) instance based on Intel SGX for workloads or Intel TDX for virtual machines (VMs).
2. Identify and enable workloads to run in these confidential computing environments. This can be done at an application level with Intel SGX (facilitated by Gramine or another client library) or at a VM level with Intel TDX.
3. Subscribe to get an Intel Trust Authority attestation key. Then insert the key into the client library on the workload (Intel SGX) or VM (Intel TDX) so it can communicate directly with the SaaS to verify the TEE.

Enabling New Use Cases in Confidential Computing

With this added layer of security, we're enabling unprecedented use cases to emerge in confidential computing.

In financial services, competitors are finding value in sharing specific information to detect fraud or money laundering, while retaining their sensitive IP. In healthcare, networks are building new AI models for early disease detection, while preserving patient privacy. These collaborations are feasible because all relying parties have assurance that the compute environment and code haven't been tampered with before they share data or run sensitive workloads.

Get Started with Intel Trust Authority

To sign up for Intel Trust Authority, please visit intel.com/trustauthority **or contact us at** trustauthority@intel.com

Learn more about Intel Trust Authority Security Solutions: https://www.intel.com/content/www/us/en/software/trust-and-security-solutions.html

Learn more about Confidential Computing powered by Intel: https://www.intel.com/content/www/us/en/security/confidential-computing.html

intel.

Printed in USA 0901/CCZ/TAN/PDF ♻ Please Recycle 355888-001US