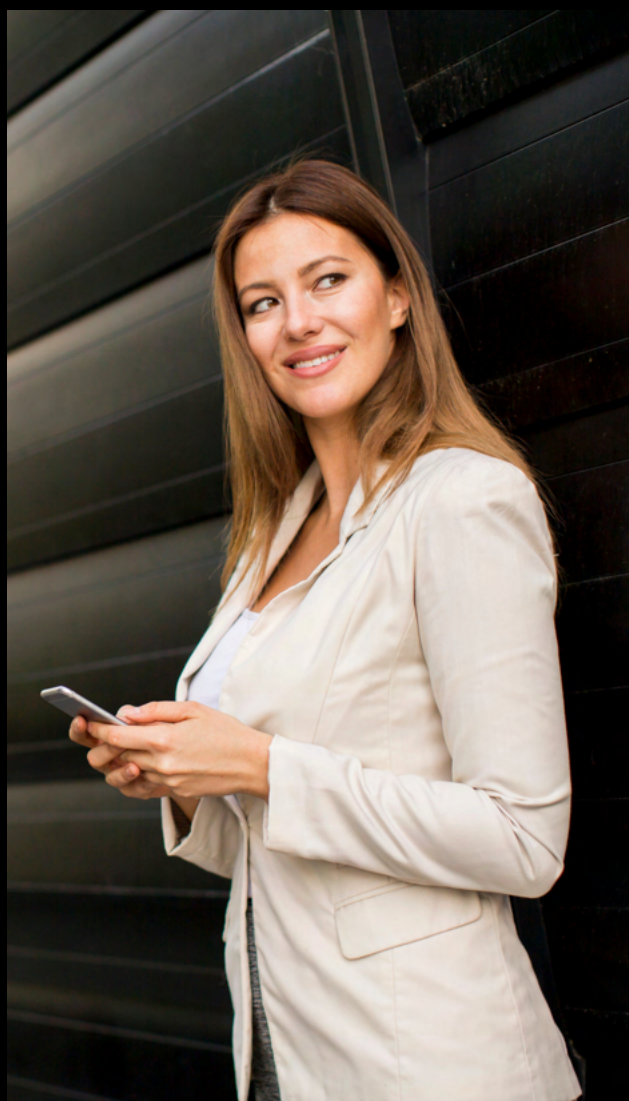
noname | accelerated by intel

Noname API Security and Intel Trust Authority



Intel's Service-Based Independent Trust Authority

Increasing Trust in Confidential Computing

As enterprises increasingly look to multi/hybrid-cloud environments, there's growing interest in a trusted third-party assurance service and new implementation of a trust authority to help build higher confidence in moving sensitive data to the cloud.

Intel Trust Authority introduces an innovative approach to objective third-party attestation.

Noname informs DevSecOps teams if what's happening right now on the public Internet API endpoints deviates from what we expected to see in the machine learning baseline and Noname points out anomalous or malicious activity with our machine learning engine by simply comparing what's happening now to the positive list that is in the baseline of what we expected to see.

Noname Active Testing tools test each new version of the API and the client applications that will be using that API prior to bringing them online on the cloud and then as your enterprise changes over time Noname Recon services provide a view of what is visible publicly on the Internet.

How does one build an Intel Xeon TDX Confidential computing encrypted Guest VM that is integrated with the Intel Trust Authority attestation service?

First boot up the Linux server with 4th generation Intel Xeon TDX Processors, then leverage the Intel Trust Authority Admin portal to request an Intel Trust Authority API key to use with the attestation API to attest that the Intel Xeon TDX CPU is genuine hardware.Inspect the contents of the JSON Web Token (JWT) response message with the JWT code to confirm that the hardware is indeed trustworthy.Inside the token is some information about this machine from the Intel Trust Authority API that the hardware is trustworthy and is authentic Intel hardware.

After attesting that the hardware is genuine, then install your API server and the Noname machine learning system software inside this trusted by TD zone where the Intel genuine CPU hardware is encrypting the guest VM memory and processor runtime.

 © Noname Security

Trusted by TD	Not Trusted by TD
Intel TDX Module	Platform Admin
Intel Authenticated Code Modules (ACM)	Discrete and integrated Devices
TD Attestation SW	All Other Software
Intel CPU Hardware	Other Platform Firmware
	Host-OS/VMM
	Bios/SMM

Figure 1 Trusted Boundaries for TDX

The next step is to create an Intel TDX encrypted confidential computing guest VM per desired cores and threads and start it up connect to it then install the software. The whole point here of putting the Noname machine learning engine inside this encrypted VM is so that what is observed with the eBPF sensor isn't leaving this encrypted memory space.

API Security

powered by **Noname machine learning AI**
on **Intel confidential Computing**

accelerated by intel

Verify the authenticity of the Noname API Security eBPF sensor and the Noname remote machine learning engine that will be analyzing the API runtime events from the containers running inside the same encrypted memory space, the Noname eBPF sensor alongside a HL7 FHIR healthcare API and a banking API also alongside the Noname machine learning engine.

 © Noname Security

More details about the service from Intel

Intel Trust Authority Decoded

Intel Trust Authority, this service is an innovative approach to objective third-party attestation. It is a SaaS-based implementation of a trust authority that provides remote verification of the trustworthiness of a compute asset based on attestation and policy.

Initially, Intel Trust Authority will verify the trustworthiness of Intel trusted execution environments (TEEs), but the vision extends to much broader device verification, like IPUs, GPUs, platform roots of trust, and beyond. Intel Trust Authority is architected as a cloud-native microservice platform running on a managed Kubernetes service, with appropriate abstractions on different cloud infrastructure platforms, on-prem, and edge locations.

Key Benefits

Independent

Verification of trustworthiness by an independent authority provides increased assurances to users, a solid security foundation for confidential computing and enables new usages in AI, multi-party compute, and federated learning.

Scalable Cloud-agnostic SaaS, multi-cloud workload support

Intel Trust Authority enables organizations to more securely scale and move workloads across a wider range of edge, on-premise, and cloud environments — all with better protection for in-use data and intellectual property.

 © Noname Security

Turnkey

Intel Trust Authority liberates enterprises from the need to build and maintain a complex and expensive attestation system. This would enable them to focus on their core business.

Intel Trust Authority is Intel's first step in creating a new multi-cloud, multi-TEE service for third-party attestation and will drive forward adoption of confidential computing for the broader industry.

Intel Trust Authority supports confidential compute workloads deployed as bare metal containers, virtual machines (VMs), and containers running in virtual machines using Intel TEEs. In the near future, support will be extended to other non-Intel TEEs in market.

How it works

1. Customer **subscribes** to the service and obtains Intel Trust Authority service API keys.
2. Customer **downloads** and integrates Intel Trust Authority Client Agent in their workload.
3. Customer **requests** TEE instantiation in the cloud (such as Azure) as normal.
4. Workload executes in the cloud after Intel Trust Authority service provides an attestation **verification token** for the TEE.

SaaS service w/ 99.95% uptime SLA

Multi/Hybrid cloud & Edge Workload support

Multi-TEE support (Initially: Intel® SGX and Intel® TDX)

Federated model for Geo-support

Provable Integrity of Verification Process

CSP agnostic & Multi-cloud deployment

 © Noname Security

> "With the introduction of Intel Trust Authority, Intel is taking confidential computing to the next level in our commitment to a zero-trust approach to attestation and the verification of compute assets at the network, edge and in the cloud."

Greg Lavender
Intel SVP CTO

About Noname Security

Noname Security is the only company taking a complete, proactive approach to API Security. Noname works with 20% of the Fortune 500 and covers the entire API security scope across four pillars — Discovery, Posture Management, Runtime Security, and API Security Testing. Noname Security is privately held, remote-first with headquarters in Silicon Valley, California, and offices in London.

nonamesecurity.com | info@nonamesecurity.com | +1 (415) 993-7371