Solution Brief

Thales and Intel Collaborate to Enhance Trust in Confidential Computing

By Enabling End-to-End Data Protection

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

intel

Background information

Confidential computing protects data in use by performing computations in an encrypted hardware execution environment, creating true end-to-end data protection when combined with data encryption at rest and in transit.

Attestation of the confidential computing environment and management of the keys injected into this environment, independent from the cloud provider and fully verifiable by regulatory bodies, are the two essential mechanisms that finally provide certifiable control back to the enterprise and full end-to-end protection of its data.

Thales and Intel are collaborating on Intel® Trust Authority attestation service to make Confidential Computing commonplace and add data protection capabilities for data in use to Thales' CipherTrust Data Security Platform. Intel announced this collaboration during their main annual event Intel® Innovation 2023, on September 19-20, in San Jose, California.

What is this collaboration about?

This collaboration enables:

- the protection of data while in use, also known as confidential computing and,
- complete customer control of their data through its entire usage cycle

Thales organically expands its CipherTrust Data Security Platform product to provide key management and encryption capabilities over a Confidential Computing environment complementing its existing market-leading solutions for data protection at rest and in motion.

Intel® Trust Authority attestation service is a cloud-provider-independent SaaS solution for Confidential Computing used to certify the authenticity of Trusted Execution Environments (TEE) and its software where the data in use is executed securely.

Independent scalable solution that provides End-to-End Data Protection for sensitive enterprise workloads:
- Intel provides the attestation that the data processing environment is authentic as expected
- Thales ensures the sensitive enterprise workloads will be encrypted at origin and will only be executed within this attested processing environment

Help comply with existing and emerging regulations on data privacy in different jurisdictions, where stringent controls are required to avoid fines

Safer cloud migration of sensitive workloads to increase confidence in the cloud deployments

What is the problem this new solution solves?

Enterprises face multiple challenges to safeguard the privacy and integrity of their sensitive workloads. In addition to security threats, they need to comply with existing and emerging data security, privacy, and resilience regulations (e.g., DORA, NIS2, GDPR, PCI, UK-PRA Prudential Regulation Authority, among others), internal security compliance policies, and manage hybrid deployment environments on premises and in multiple clouds.

One of those challenges is migrating sensitive workloads to be computed in the cloud securely. Confidential Computing protects data while in use. Computations on data are performed in a cryptographically isolated hardware-based Trusted Execution Environment (TEE), removing, or reducing the ability for a rogue operator at a cloud provider to access code and data while being executed. A weakness of most current deployments of Confidential Computing is that the cryptographic material that verifies the Confidential Computing environment and controls the workload protection is managed natively by the cloud provider without proper separation of duties.

Separation of duties is an important security principle when the responsibility is shared between the enterprise and the cloud provider. While most cloud providers offer native data protection features, the Shared Responsibility Model dictates that the ultimate onus of safeguarding sensitive data rests with the enterprises/organizations. Therefore, separation of duties is considered a best practice to help avoid security or privacy incidents and errors. For example, when managing keys in the cloud, many customers require a separation of duties between their encryption key management and the management of sensitive data stored in the cloud to comply with data sovereignty requirements. In response, Thales and its cloud provider partners have co-innovated to develop Bring Your Own Key (BYOK) and Hold Your Own Key (HYOK) services. Similarly, the certification (attestation) of Confidential Computing secure enclaves should not be done by the cloud provider within the cloud provider environment. The joint solution from Thales and Intel enables enterprises/customers to remain in control of their data protection, ensuring that sensitive workloads are never decrypted outside of a genuine certified Confidential Computing secure enclave enabling End-to-End Data Protection.

This collaboration between Thales and Intel enables advanced customer controls around Confidential Computing use cases, such as End-to-End Data Protection — for data protection at rest, in motion, and in use — to secure customers' sensitive workloads on premises, during its migration to the cloud, and in the cloud for storage and processing, while allowing the enterprise to stay in control of their data thereby separating this role from the cloud provider. Separation of duties (control) is especially important for highly regulated industries, the public sector, national security, and other verticals where data protection is paramount to safeguard the privacy of the information.

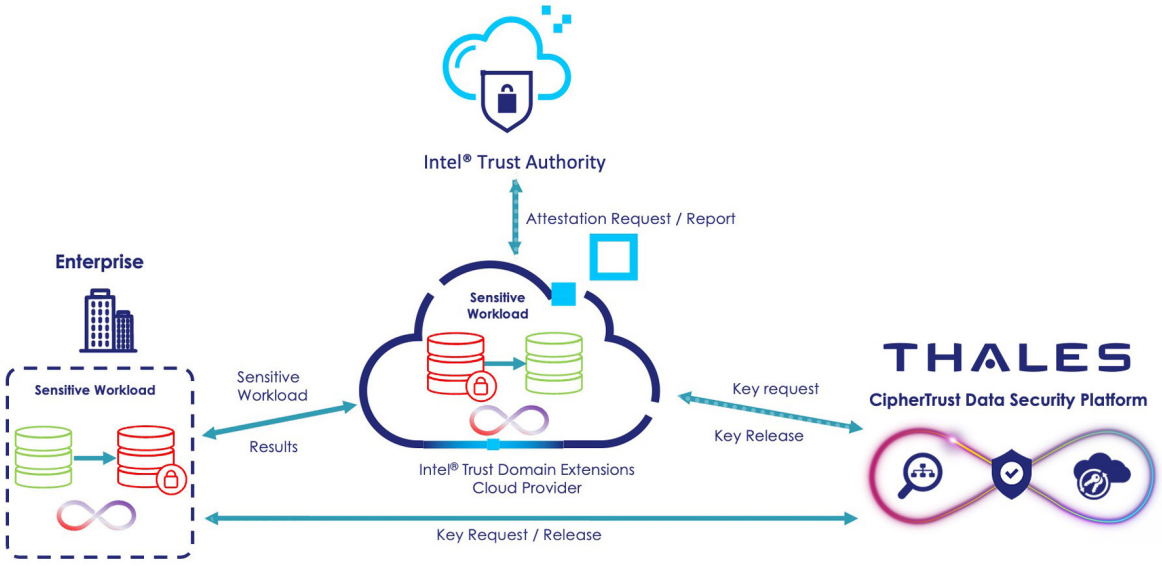
How does end-to-end data protection work?

- The sensitive workload is initially encrypted within the enterprise data center using the Thales CipherTrust Data Security Platform. The encrypted workload is ready to be shared and migrated to the cloud.
- When the enterprise/customer executes this workload and performs some computation on the confidentially shared datasets, a request from the Confidential Computing enclave is sent to start processing. At this point, Thales CipherTrust Manager requests attestation from the Intel® Trust Authority (attestation service) to certify the genuineness of the Intel Confidential Computing TEE enclave/code and initiates the key release from CipherTrust Manager to decrypt the Workload for execution and computation.

A use case

Confidential multi-party collaboration refers to customer scenarios for Confidential Computing where different parties may security "share" and collaborate on datasets and workloads to get results while preserving their privacy, confidentiality and simultaneously complying with privacy regulations.

- In healthcare, to facilitate the diagnosis of diseases and the development of pharmaceutical drugs, hospitals and healthcare facilities can contribute patient datasets to train a machine learning model. Each facility that contributes to training the model can use it and receive useful results without seeing the other party's sensitive data.
- In banking, multiple banks can share data without exposing their customers' personal data to detect money laundering. Banks run analytics on the combined sensitive data set that can detect the movement of money by one user between multiple banks without the banks accessing each other's data.



End-to-End Data Protection

Enhancing trust in Confidential Computing

cpl.thalesgroup.com

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us