Google Cloud | inabit.

Inabit offers high-security management for cryptocurrency with Trusted Computing technology

November 2024

inabit.

An advanced, highly secure platform for managing digital assets and cryptocurrencies.

Inabit caters to businesses and institutions using digital wallets and offers robust solutions for corporate governance, reporting, API integration, and profile management.

To ensure maximum crypto wallet security, the private keys guarding the wallet must remain confidential and never be exposed. Inabit achieves this by utilizing Google Cloud Confidential Space, a Trusted Execution Environment (TEE), which is built based on AMD Secure Encrypted Virtualization (SEV) hardware.

Confidential Space safeguards sensitive data and operations by creating an isolated, secure environment on Google's public cloud, delivering unparalleled protection.

In addition, Inabit's Trusted Computing Mechanism (TCM) technology ensures that private keys can only be accessed inside the Confidential Space, meaning no one can reach them - not even Inabit. The company utilizes the robust security infrastructure provided by Google and AMD to offer the most reliable layer of protection.

For decades, leading banks, defense organizations, and governments have relied on hardware-based solutions for their most sensitive and secure operations. Now, Inabit brings these trusted capabilities to all businesses by implementing TCM. This enables Inabit's customers to securely conduct large-scale cryptocurrency transactions, confident that their assets are always protected. Subsequently, Inabit can expand its services to more customers without compromising security.

Self-custody solution powered by advanced hardware encryption

Inabit also provides customers with a self-custody solution, enabling them to retain complete control of their digital assets by holding access to them locally. This approach stands in contrast to custodial services offered by many other providers, where control of the customer's assets resides with the exchange or service.

The theft or misuse of users' keys, or being able to sign on fraudulent transactions are big issues in cryptocurrency-based services and can lead to significant financial loss and reputational damage for businesses that rely on cryptocurrency as a primary way of payment.

To mitigate these issues, Inabit's digital asset management service prioritizes the security of these user keys, ensuring they always remain encrypted. To achieve this, Inabit employs a solution that allows customers to securely sign transactions with their private keys without exposing them at rest, in transit, or even in processing.

Deliver a reliable service

To further enhance their service's security, Inabit selected Google Cloud's Confidential Computing platform, leveraging Google's advanced security measures and industry-leading practices.

When deploying secure instances in this cloud environment, Inabit guarantees that neither external parties nor Inabit itself can interfere with or modify the code or data. The hardware upholds this security, with the CPU encrypting the memory to ensure the highest level of protection.

Dr. Moti Geva, inabit's CTO, spearheaded the evaluation and implementation of Google Cloud's Confidential Computing platform. "Google's solution surpasses other solutions we looked into in cryptographic strength and ability to verify our TCM workload," he stated. "We can effectively mitigate many security vulnerabilities by having our Trusted Computing Mechanism (TCM) integrated with Google's Confidential Space."

Geva also noted that critical vulnerabilities have already been discovered in digital wallets that use various cryptographic technologies available in other solutions currently on the market. "These issues require digital asset companies, which improperly implement these secure protocols, to deploy urgent security fixes—a risk we are making an effort to mitigate by having many risks secured by Google and AMD," he added.

GCP and its Confidential Space product serve as both a cloud provider and a security partner for Inabit, enabling the company to deliver a trusted, reliable, and scalable service to its customers in the digital assets market.

"We use standard and well-tested cryptography that has been in use for decades and used across all industries," said Geva, "So it's a key issue for us to have a partner who can provide and support it. The strong cryptography protects the users' keys. GCP's Confidential Space implementation is more robust than other solutions in the market and likely less vulnerable to new attacks. It has a very large commercial and open source community behind it to mitigate and quickly solve issues when they arise."

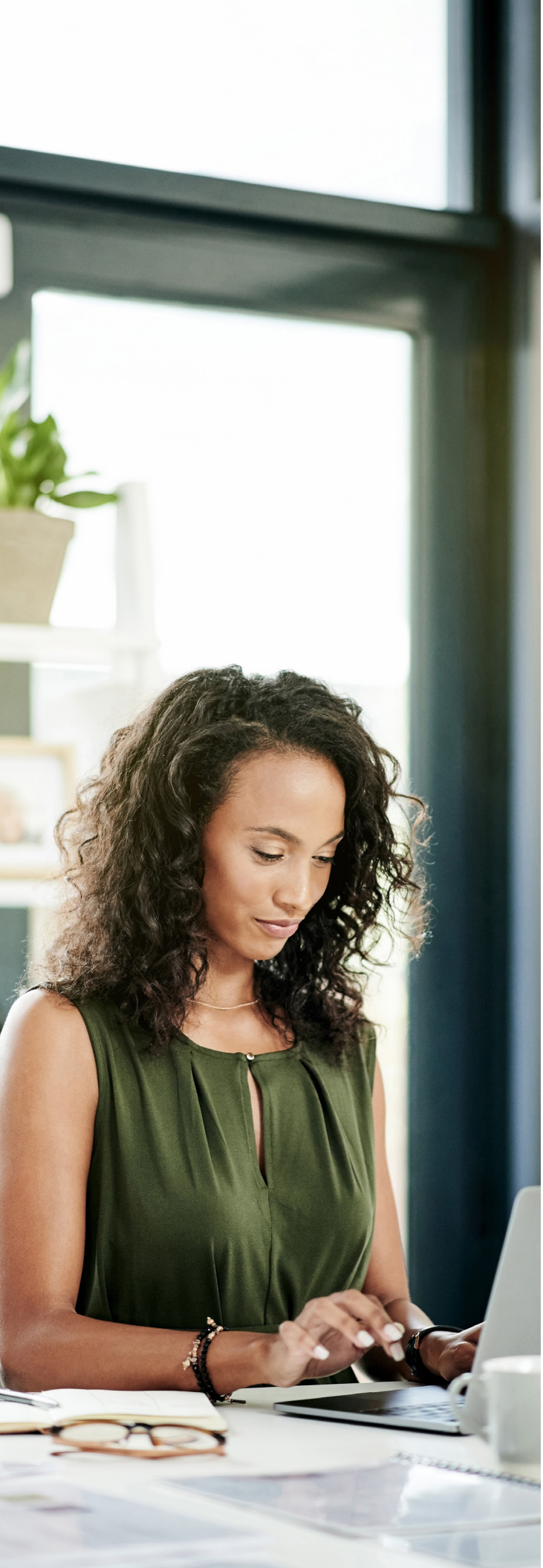
Secure transactions and trusted code attestation

When selecting a cloud service, Inabit prioritized a container environment that was easy to develop for and set up, which allowed for easy and straightforward communication between enclaves and the outside environment without requiring code modifications.

A key part of Inabit's process raised a need to allow for remote code attestation by Google, i.e., Google is able to attest which code is being securely executed inside the Confidential Space Inabit can remotely verify that the code is both secured inside a TCM and is indeed the expected workload. "This is a significant differentiator for us," said Geva. "We worked with Google's Confidential Space product team on this, and it can enhance the security of our product and strengthen the trust we build with our customers."

Inabit has been collaborating with Google for over a year, and the implementation process is now reaching its peak. This already enabled Inabit to actively enforce its policy layer within the enclave so each signatory and customer can securely manage their private keys and authorize transactions within their organizations.

The infrastructure provided by Google and implemented by Inabit enables the company to securely process blockchain transactions within the enclave, ensuring that sensitive keys remain completely inaccessible —not just to external threats but even to Inabit's own super users or any other internal actors. This exclusive solution provides a critical layer of protection.



Seamless integration

Geva is confident in his decision to use Confidential Computing. "It seamlessly integrates into our CI/CD process for development, providing ease of use in attesting to the secure workload within the TCM," he explained. It also enables us to scale horizontally with relative ease, allowing us to add more machines, process an increasing number of transactions, and serve more customers."

According to Geva, Confidential Space addresses all of Inabit's essential requirements: "It allows us to use standard containers and code, which is highly beneficial for our developers, as they can continue using familiar methods. It protects our system from unauthorized access, including insiders, mitigating the risk of bad actors compromising the system or accessing customer keys and transactions.

Moreover, it enables the third-party attestation of the workload, a critical factor that allows us to delegate trust in what's being executed to a trusted partner like Google. This is instrumental in building trust with our customers, ensuring that the workload is securely attested and that their keys, assets, permissions, and transactions are safe and enforced."

With this integration, customers from various segments are joining Inabit's service and performing transactions in increasing volumes, which reflects their trust in the system supported by GCP. They conduct transactions in a wide range of cryptocurrencies on the blockchain, create policies, perform swaps, and convert cryptocurrencies to fiat and vice versa — all in a simple, easy, and, most importantly, secure manner.

Google Cloud