METACO Leverages IBM Cloud and Confidential Computing Capabilities to Help Secure its Integrated Digital Asset Management Solution

Zurich and Lausanne, Switzerland - March 25, 2021– Today IBM (NYSE: IBM) and METACO, a provider of security-critical infrastructure that helps large banks manage digital assets, announced that METACO will leverage confidential computing capabilities through IBM Cloud and IBM Cloud Hyper Protect Services for their digital asset orchestration system. With its platform running on IBM Cloud, METACO can deliver its traditional finance clients benefits including increased security and scalability as they adopt hybrid cloud strategies.

To address the rapidly growing market demand for digital assets, METACO enables large financial institutions to securely integrate cryptocurrencies, tokens, and distributed ledger use-cases into their core infrastructure. METACO's unique offering for digital asset custody, transaction management, trading, and tokenization has made it a sound solution for banks and exchanges.

To support the requirements of clients in highly regulated industries such as banking and financial services, METACO leverages 'Keep Your Own Key' (KYOK) encryption and confidential computing capabilities from IBM. This solution allows METACO's clients to retain sole access to their crypto keys,[1] meaning by engineering design, IBM does not have access to clients' keys. These enhanced security capabilities help clients mitigate the risk of malicious actors manipulating workflows, viewing confidential data or getting access to assets. Additionally, clients can choose where to run their solution - whether in the cloud, on premises or in a hybrid cloud environment.

METACO's solution for safe custody of digital assets, offers new options of wallet deployments for flexibility of hot, warm, cold, nearline and frozen storage of digital assets, each encompassing a specific balance of security and agility to best fit the needs of institutions. The orchestration system is running in IBM Cloud Hyper Protect Virtual Server enclaves, which provide access to IBM's confidential computing capabilities.

Adrien Treccani, CEO and Founder of METACO commented, "IBM is one of the financial industry's longest standing and most trusted technology providers, and we are proud to join forces to strengthen the offering of our custody solution and digital asset orchestration system for institutions. At METACO, we are constantly striving to innovate, expand and improve upon our service offerings. This integration will allow us to deliver greater levels of security and trust to our clients as they innovate in the digital asset space."

"As the world's leading financial institutions adopt hybrid cloud, it is critical that they keep in mind security and privacy assurance," said Hillery Hunter, IBM Fellow, VP and CTO, IBM Cloud.

"As companies such as METACO continue to help the world's top banks and exchanges manage their digital assets, IBM's confidential computing capabilities help its clients ensure their data and processes are managed securely, bringing trust into the ecosystem and providing privacy assurance".

IBM Cloud Hyper Protect Services are available on IBM Cloud and on-premises via IBM LinuxONE, delivering the highest level of commercial privacy assurance available today.

About METACO

METACO is the leading provider of security-critical infrastructure enabling financial institutions to enter the digital asset ecosystem. The company is trusted by top banks, exchanges and infrastructure providers globally.

Founded in 2015, METACO brings together a diverse team of industry specialists in software, security, cryptography and banking to transform the financial services industry. The company is deeply integrated into the banking sector through a growing network of strategic partners and institutional shareholders.

About IBM

To learn more about IBM Cloud, visit:www.ibm.com/cloud/

Contacts:
Hannah Slocum
IBM Communications
hslocum@us.ibm.com

[1] Only clients or their trustees control their assets—not METACO, nor IBM. Clients are issued special IBM smart card HSMs (FIPS 140-2 Level 3) to ensure the root of trust. During a trusted key ceremony, these smart cards collectively generate AES256 bit key parts that are securely transferred to the platform's HSM and assembled into a master wrapping key inside an isolated HSM (FIPS 140-2 Level 4) domain. Only the client retains control of their master wrapping key. HSM domains are highly isolated and protected by 360-degree envelope tamper detection and response.

Additional assets available online: Photos (2)

Video (1)

https://stage.mediaroom.com/ibmnewsroom/2021-03-25-METACO-Leverages-IBM-Cloud-and-Confidential-Computing-Capabilities-to-Help-Secure-its-Integrated-Digital-Asset-Management-Solution