VICOM Infinity

Vicom Infinity Solution Whitepaper: IBM Hyper Protect Digital Asset Platform

Yongkook(Alex) Kim
IBM Z/Blockchain Champion

When bitcoin was first introduced, crypto-currency and blockchain technology were thought to be somewhat interchangeable. As the industry and community matured and better understood crypto-currency and blockchain uses, it became clearer that indeed they have different purposes. Blockchain on the enterprise side has been adopted as a distributed ledger, and a great example is the Linux Foundation's Hyperledger project.

Crypto currencies have been more like the wild-wild-west, where a lot of 'me-too' spinoffs from bitcoin currency had attracted many investors worldwide. As individuals, private sectors as well as governments acknowledged this type of alternative currency will exist for long time, and many architectures and practical implementations have been proposed to protect digital assets such as crypto currencies. IBM recently announced Hyper Protect Digital Assets Platform, which utilizes IBM LinuxONE's very strong security features to protect those digital assets against any intrusions.

1. What is Digital Asset and why is it important

As many of us know already, bitcoin was developed by Satoshi Nakamoto as a way of peer-to-peer electronic cash transactions. He noticed the problems of electronic payment systems and wanted to solve the issue with his invention of a peer-to-peer distributed transaction system, without any central authority being involved. Over ten years passed since bitcoin's genesis block was created, then many other crypto currencies were introduced, and disappeared too. Many crypto-currency-related businesses have been founded and one popular area was crypto currency exchanges - where you can convert central bank managed currency into a crypto currency and vice versa. There have been some incidents with crypto wallets being stolen, or even an owner of the crypto currency exchange passing away and no one else knew the master encryption key for the crypto currency asset repository.

Now imagine today that similar things can happen to you even if you do not own any crypto currencies. If you use any coffee/espresso franchise app, they may have their own rechargeable wallets either in your local currency value or their own points value translated from the local currency. If something happens to their system that stores your money/points and loses them, there is almost nothing your central bank and/or local bank can do as it is out of the 'governed/regulated' system. After you have made the purchase of points, it's a completed transaction from their point of view.

As another example, let's take a look at application-based money transfers. More and more banks are permitting people to transfer money to other banks using their own franchised money transfer applications. You just need the recipient’s email or phone number. You no longer need the bank routing/account number to do a wire transfer. Some countries use their wireless phone company to manage money transfer and make payments, bypassing banks altogether. There are many online payment companies that enable using applications to charge central currency into the central system and make payments/transfers to anyone using the same application. You can think of all of these options as 'digital assets', where the valued asset is stored in digital format and can be moved from one owner to another easily and quickly without having to involve the 'traditional' central agency. Digital assets are not just currency but also anything that represents ownership of physical assets someone or an organization can own legally - such as property titles or deeds transformed into digital format (that might contain digital signatures), or even intellectual property that does not even have any physical properties. If any bad incidents (including cyber-attacks) happen to a system that stores these digital assets such as deeds, it can be catastrophic if there is no other way to restore proof-of-ownership and/or the property itself.

Many countries, including the U.S, are putting effort into understanding how 'CBDC - Central Bank Digital Currency' would work for them and how to properly prepare for the next generation of currency exchanges and safeguarded infrastructures. If/when a central bank announces a plan for digital currency, it would make a huge impact to existing private banks and accompanied payment systems. Since it has the potential of adopting Satoshi Nakamoto's idea of peer-to-peer payment system, it is critical to understand how a digital asset exchange enterprise can assure their infrastructure is safe and secure.

IBM's Hyper Protect Digital Asset Platform can provide the highest level of security and safeguards for the services handling those digital assets. Let's take a look how the proposed architecture with Hyper Protect Digital Asset Platform works.

2. Why Use Hyper Protect? - Proposed Solution Architecture

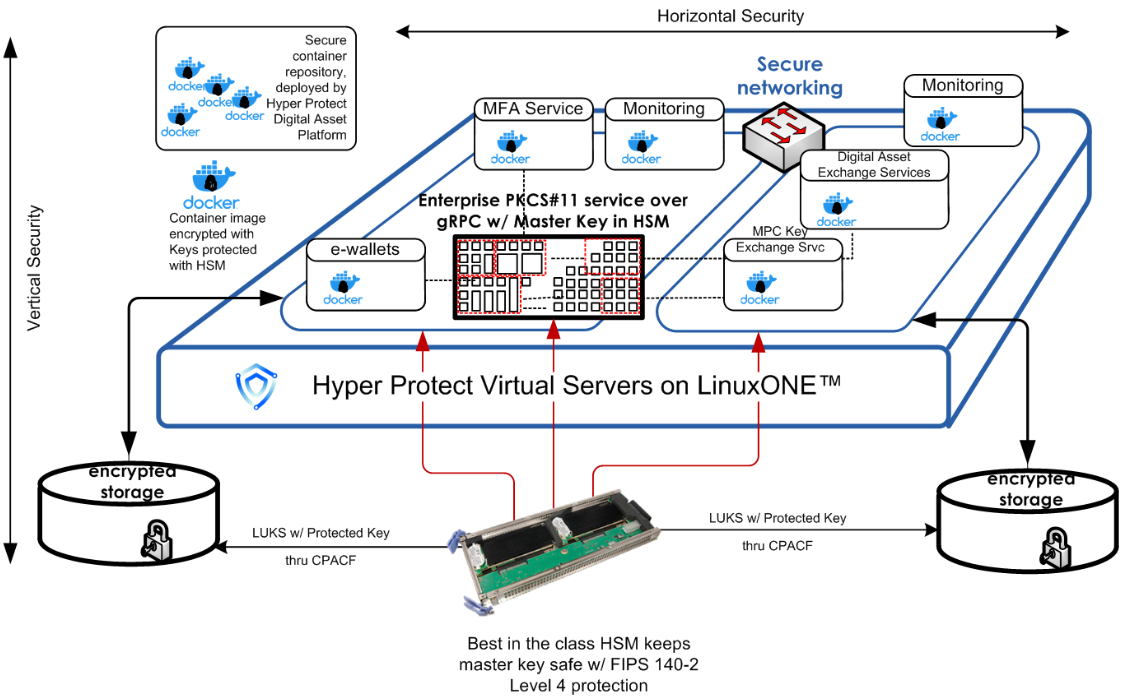
Root of Trust - keeping master key secure

The IBM LinuxONE system offers a very strong hardware security module (HSM) known as the Crypto Express adapter (CEX). Using CEX, Hyper Protect Crypto Services enables you to keep and manage operational encryption keys very secure as follows. These operational keys are encrypted with your own master key that is only visible to you only when entering them, and never leaves the hardware, i.e. the HSM CEX in the LinuxONE. The master key(s) can be backed up using smart cards thru another strongly secured service called TKE (Trusted Key Entry) as described in chapter 3. This master key management with encrypted operational keys provides the 'root of trust' to make Hyper Protect Digital Asset Platform most secure.

You can read more about the highest security provided by IBM LinuxONE in the IBM Redbook : Maximizing Security with LinuxONE
http://www.redbooks.ibm.com/abstracts/redp5535.html?Open

Providing secure application hosting server – Vertical security

Now, the digital asset management application (let's call it digital wallet application or “hot wallet”) will be running on LinuxONE's Hyper Protect Virtual Server. This server will boot up with a tamper resistant secure boot process, and the storage accessed by the virtual server will be encrypted with a protected key. This protected key is only decrypted in a special memory area of LinuxONE. When access to the encrypted disk is needed, the system then executes encryption/decryption of data transferring in and out of the disk.


Horizontal Security
Vertical Security
Secure container repository, deployed by Hyper Protect Digital Asset Platform
docker
docker
Container image encrypted with Keys protected with HSM
MFA Service
Monitoring
Secure networking
Monitoring
Digital Asset Exchange Services
Enterprise PKCS#11 service over gRPC w/ Master Key in HSM
e-wallets
MPC Key Exchange Srvc
Hyper Protect Virtual Servers on LinuxONE™
encrypted storage
LUKS w/ Protected Key
thru CPACF
LUKS w/ Protected Key
thru CPACF
encrypted storage
Best in the class HSM keeps master key safe w/ FIPS 140-2 Level 4 protection

<Figure 1. Highly simplified deployment example of Hyper Protect Digital Asset Platform>

Once the server is up, it will deploy a container image that is also encrypted and signed by the 'Secure Build' process. During the build process of the secure Docker container (or equivalent OCI compliant container) images, many security checks and endorsements will be performed to make sure there will be no malicious code being implanted, as well as the application code saved in the container is legitimate, from the software vendor. In this case it would be the digital wallet application.

If there is any reason to capture the memory dump from Hyper Protect Virtual Server for debugging purposes, the dump will also be encrypted. In turn, one would have to have a private key to access the encryption key for the memory dump. This capability is definitely key differentiator for LinuxONE compared to other platforms.

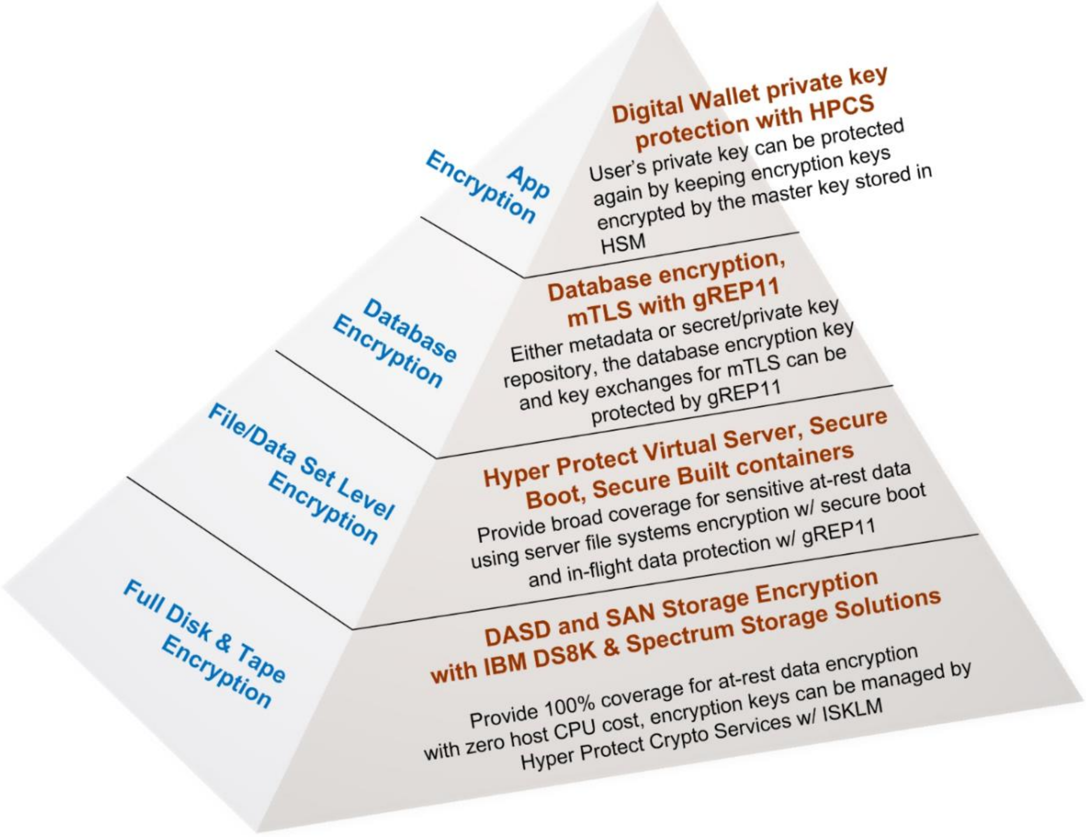
Communicating between container images using secure channel – Horizontal security

Since Hyper Protect Virtual Server can limit the login access to the OS shell, the server would communicate externally only with APIs. There could also be secure communication channels between application containers using secure protocols such as TLS or IPSec. The asymmetric key pairs for applications and APIs would be managed by EP11 over RPC (GREP11) where the master key for EP11 service would also be coming from the HSM(Crypto Express card), thus providing maximum protection of asset transfers when the digital asset is transferred using the end-user's private/public key pair. If the digital wallets need to be a cold wallet, then the master key stored in HSM would be nullified to make all the assets inaccessible. The cold wallet can be accessed again once the master key restoration ceremony is completed.

What problems does the Hyper Protect Digital Asset Platform solve?

Completing the picture of Pervasive Encryption Pyramid for LinuxONE

Either from external or internal threats, the security of applications needs to be protected from all possible accessible threats by bad actors. What Hyper Protect Digital Asset Platform architecture provides is maximum security protection of every layer that any security professional would demand. When IBM LinuxONE was designed, it was proposed to achieve maximum security with architecture called Pervasive Encryption. Pervasive Encryption addresses protection from many threats by encrypting data in-transit and at-rest based on FIPS 140-2 Level 4 HSM module. Hyper Protect Digital Asset Platform architecture is an excellent example of how enterprise applications can achieve Pervasive Encryption with LinuxONE.


App Encryption
Digital Wallet private key protection with HPCS
User's private key can be protected again by keeping encryption keys encrypted by the master key stored in HSM
Database Encryption
Database encryption, mTLS with gREP11
Either metadata or secret/private key repository, the database encryption key and key exchanges for mTLS can be protected by gREP11
File/Data Set Level Encryption
Hyper Protect Virtual Server, Secure Boot, Secure Built containers
Provide broad coverage for sensitive at-rest data using server file systems encryption w/ secure boot and in-flight data protection w/ gREP11
Full Disk & Tape Encryption
DASD and SAN Storage Encryption with IBM DS8K & Spectrum Storage Solutions
Provide 100% coverage for at-rest data encryption with zero host CPU cost, encryption keys can be managed by Hyper Protect Crypto Services w/ ISKLM

<Figure 2. Pervasive Encryption Pyramid with Hyper Protect Digital Asset Platform>

3. Solution Offering and Deployment Examples

IBM Hyper Protect Digital Assets Platform – Soft Bundle Offering

The IBM Hyper Protect Digital Assets Platform is a trusted computing base (TCB) for digital asset custodians, exchanges, issuance providers, and permissioned blockchains solutions and hardened operational processes that, taken together, provide a high degree of confidence for their customers.

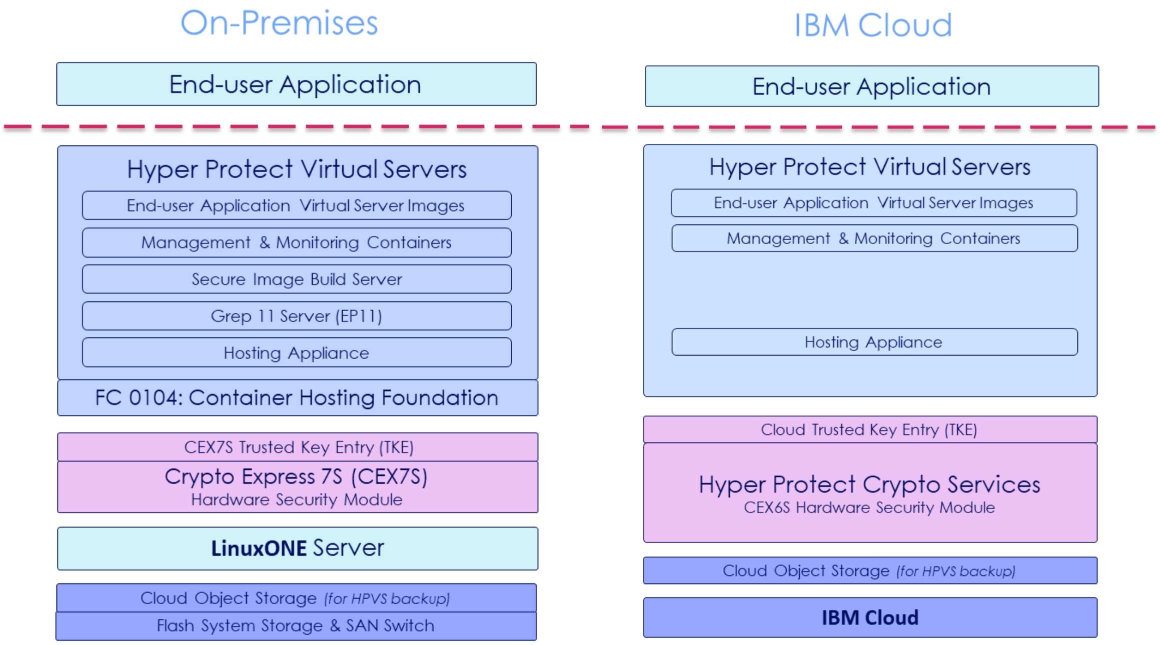
There are many LinuxONE clients that deployed Hyper Protect Digital Asset Platform. You can find a good executive summary of the Hyper Protect Digital Asset Platform posted here: https://www.ibm.com/blogs/systems/hyper-protect-your-business-for-digital-transformation

To name a few, Hex Trust (www.hextrust.com) is a Fintech startup migrating a production institutional digital asset custody solution to an on-prem custody-as-a-service. OnChain Custodian (www.oncustodian.com) is a Fintech startup using IBM Cloud Hyper Protect Crypto Service to offer cloud-based institutional digital asset custody. Kore Technologies(www.kore-technologies.ch) is a Fintech startup based in Switerland offering an on-premise and cloud-based enterprise-grade digital asset custody and issuance solution. DACS(www.securedacs.com) is a Fintech startup located in South Korea building on-prem LinuxONE native institutional digital asset self-custody and trading solutions.

CONTACT US

To learn more on Hyper Protect Digital Asset Platform, please contact us at: info@vicominfinity.com or 631-694-3900

To learn more about Vicom Infinity, please visit our website at VicomInfinity.com


On-Premises
End-user Application
Hyper Protect Virtual Servers
End-user Application Virtual Server Images
Management & Monitoring Containers
Secure Image Build Server
Grep 11 Server (EP11)
Hosting Appliance
FC 0104: Container Hosting Foundation
CEX7S Trusted Key Entry (TKE)
Crypto Express 7S (CEX7S)
Hardware Security Module
LinuxONE Server
Cloud Object Storage (for HPVS backup)
Flash System Storage & SAN Switch
IBM Cloud
End-user Application
Hyper Protect Virtual Servers
End-user Application Virtual Server Images
Management & Monitoring Containers
Hosting Appliance
Cloud Trusted Key Entry (TKE)
Hyper Protect Crypto Services
CEX6S Hardware Security Module
Cloud Object Storage (for HPVS backup)
IBM Cloud

<Figure 3. Hyper Protect Digital Asset Platform Solution Options>