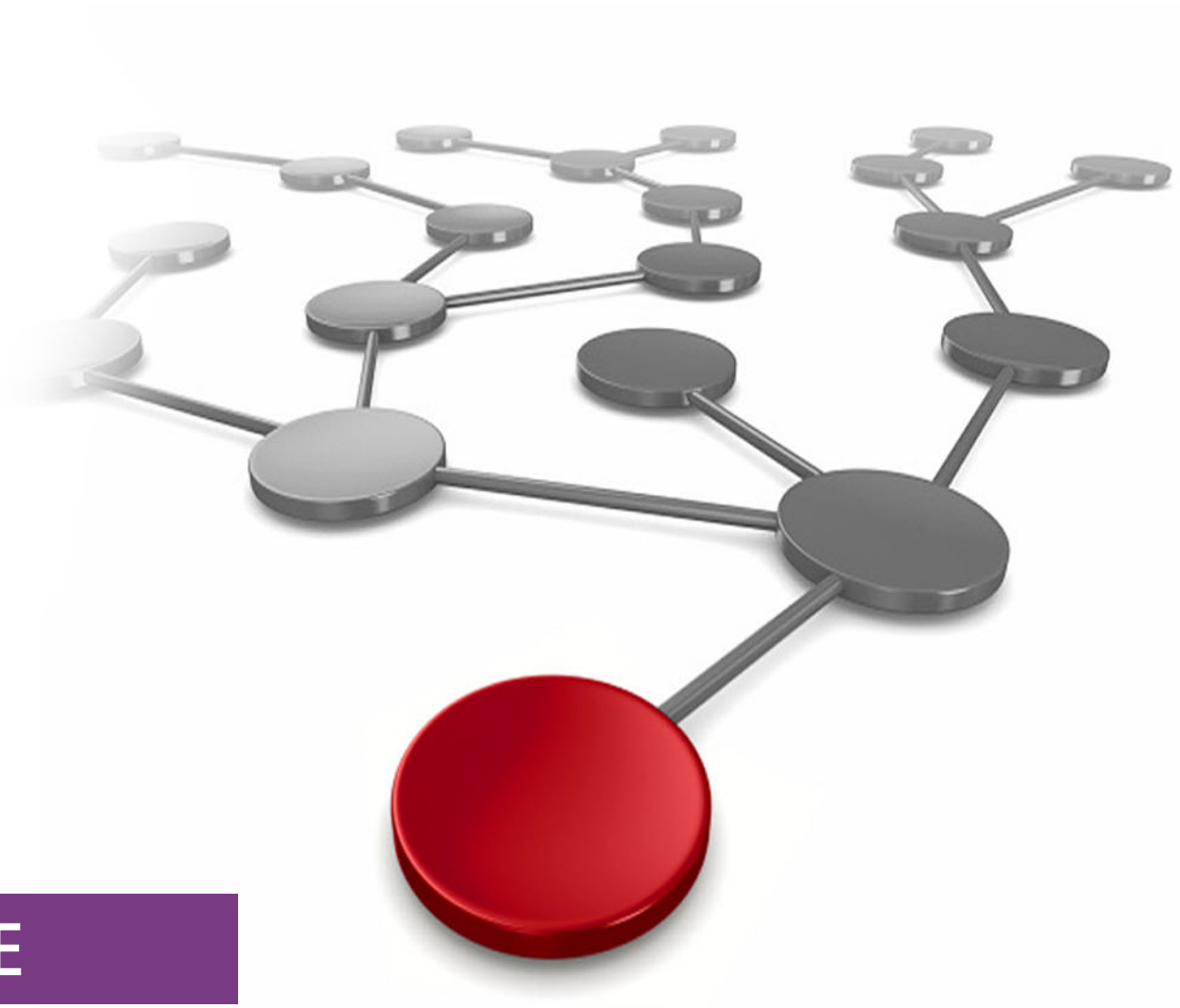
Redbooks
ibm.com/redbooks

Maximizing Security with LinuxONE

Lydia Parziale
Leticia Alexander
Yongkook Kim
Rushir Patel
Narjisse Zaki



LinuxONE

IBM

Redpaper

IBM Redbooks

Maximizing Security with LinuxONE

August 2020

REDP-5535-01

Note: Before using this information and the product it supports, read the information in “Notices” on page v.

Second Edition (August 2020)

This edition applies to LinuxONE, 2020.

This document was created or updated on August 10, 2020.

Contents

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

Db2®	IBM Cloud®	RACF®
DS8000®	IBM Cloud Pak®	Redbooks®
FICON®	IBM Security™	Redbooks (logo) ®
IBM®	IBM Z®	z/VM®

The following terms are trademarks of other companies:

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Java, and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

OpenShift, Red Hat, are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.

Preface

LinuxONE® is a hardware system that is designed to support and use the Linux operating system based on the value of its unique underlying architecture. LinuxONE can be used within a private and multi-cloud environment to support a range of workloads and service various needs.

On LinuxONE, security is built into the hardware and software.

This IBM® Redpaper® publication gives a broad understanding of how to use the various security features that make the most of and complement the LinuxONE hardware security features, including the following examples:

- Hardware accelerated encryption of data, which is delivered with near-zero overhead by the on-chip Central Processor Assist for Cryptographic Function (CPACF) and a dedicated Crypto Express adapter.
- Virtualization and industry-leading isolation capabilities with PR/SM, EAL 5+ LPARs, DPM, KVM, and IBM z/VM®.
- The IBM Secure Service Container technology, which provides workload isolation, restricted administrator access, and tamper protection against internal threats, including from systems administrators.
- Other technologies that use LinuxONE security capabilities and practical use cases for these technologies.

This publication was written for IT executives, architects, specialists, security administrators, and others who consider security for LinuxONE.

Authors

This paper was produced by a team of specialists from around the world working at the IBM Redbooks Center, Poughkeepsie.

Lydia Parziale is a Project Leader for the IBM Redbooks® team in Poughkeepsie, New York, US, with domestic and international experience in technology management, including software development, project leadership, and strategic planning. Her areas of expertise include business development and database management technologies. Lydia is a certified PMP and an IBM Certified IT Specialist with an MBA in Technology Management and has been employed by IBM for over 25 years in various technology areas.

Leticia Alexander is an IT architect and founder of a startup in Atlanta, Georgia, US. Leticia started her career with IBM as a Sales Software Technical Specialist for the IBM Z® platform where she conducted software solutions designs and configurations and participated in POCs with customers. She worked on IBM's Sales Team for the AT&T account as a Sales Specialist selling IBM Storage, IBM Z, and Power Technology. She has conducted research and development on Cyber Security for High Performance Computer and Cloud workloads per a SBIRS grant with the Department of Energy. She enjoys working with IBM Z Technology customers to modernize the Z Platform to fit use cases, such as Blockchain, Cloud, and AI. Leticia's area of expertise is Cyber Security, Blockchain, AI/Data, and cloud technologies. She has a Bachelor Degree in Finance from Georgia State University.

Yongkook Kim is an engineer and architect with over 20 years of industry experience. Yongkook started his career as a design engineer for IBM Z Crypto HW at IBM Poughkeepsie, New York, US, in 2001, and designed AES engine in ASICs for Crypto Express 2. He then joined IBM sales team for Wall Street to assist financial sector clients with IBM Z technology. He has been a technical advisor for IBM Z clients in NY Metro area since 2007 and participated in multiple benchmarks with international teams as well. Yongkook joined Vicom Infinity, a premiere IBM Business Partner in 2014 as a Solutions Architect. He actively participated in PoCs and solution designs with various industry clients and enjoys adopting new technologies, such as blockchain, voice assistants, and IoT into enterprise solutions, such as LinuxONE. Yongkook holds Masters degree from NYU Polytech School of Engineering.

Rushir Patel is an IBM Offering Manager for LinuxONE based in Raleigh, North Carolina, US. He has over 8 years of experience in technology product management, agile software development, and UX research and design. His areas of expertise include cyber security, enterprise data management, and cloud computing technology. He has an MBA from the University of North Carolina Kenan-Flagler Business School and a BSc Electrical Engineering from North Carolina State University.

Narjisse Zaki is an IT Architect in IBM ATS. She provides pre-sales technical support for Linux consolidation projects on Linux on Z and LinuxONE across EMEA countries, and more recently, she supports Red Hat OpenShift engagements. She is based in Montpellier, France. Narjisse is also the engagement leader for LinuxONE pre-sales activities in MEA at the IBM Systems Center, Montpellier. In past years, Narjisse supported Oracle consolidation projects within the European IBM Oracle Center (IOC). Before joining the IOC, Narjisse was involved in Agile Project Management leading projects as a Scrum Leader. She has been an international speaker in several conferences and events around the world. She holds a M. Engineering in Computer Science and Management.

Thanks to the following people for their contributions to this project:

Robert Haimowitz
IBM Redbooks, Poughkeepsie Center

Edi Lopes Alves
IBM Brazil

Guillaume Hoareau, Sylvain Carta
IBM France

Dr. Reinhard Bündgen, Stefan Raspl, Pradeep Parameshwaran, Tony Gargya
IBM Germany

Alixander Laffredo-Dietrich, Jin VanStee, Rebecca Gott, Brett Webb, Anthony Sofia, Todd Arnold, Richard Kisley
IBM USA

Tom Amodio
President, Vicom Infinity, Inc.

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an IBM Redbooks residency project and help write a book in your area of expertise, while honing your experience with leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies last from 2 to 6 weeks, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks

- Send your comments in an email to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, IBM Redbooks
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:

  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

1

Introduction

At IBM, we believe that your data is yours – and yours alone[1]. The insights and advantages that come from your data are yours to use in the pursuit of your business objectives. IBM is dedicated to this mission, and our LinuxONE platform was designed around this core statement.

The world is experiencing a time of exponential growth in the sheer volume of data, fueled by the digital transformation of systems, services, and interconnected devices that all require strong data serving capabilities. Businesses must manage, store, and most importantly, protect this information while they use it to gain competitive advantage.

IBM LinuxONE is an all-Linux enterprise platform for open innovation that combines the best of Linux and open technology with the best of enterprise computing in *one* system.

In this IBM Redbooks publication, we explore the features and capabilities of the LinuxONE platform that extend enterprise-grade security to the Open Source world.

This chapter includes the following topics:

[1] https://www.ibm.com/watson/data-privacy/

1.1 Introduction to LinuxONE

Linux adoption grew dramatically over recent years, expanding from initial use by startups for web servers into its use today for a vast range of enterprise computing workloads. It grew up alongside the open source community, which is a unique resource that uses a network of passionate and dedicated developers who are willing to contribute to various projects.

IBM LinuxONE is an all-Linux enterprise platform for open innovation that combines the best of Linux and open technology with the best of enterprise computing in ONE system. It is designed to support customers who want an efficient and cost-effective solution for protecting their data and hosting various enterprise-grade Linux workloads. The LinuxONE platform is defined by security, speed, scalability, reliability, and openness.

LinuxONE's hardened Linux-based software stack can run most open source software packages, such as databases and data management (that is, MariaDB, PostgreSQL, MongoDB, and Apache Spark), virtualization platforms, and containers (IBM z/VM, KVM, Docker, and Podman), automation and orchestration software (Kubernetes, OpenStack, Puppet, Node.js, Juju, and Chef), and compute-intensive workloads, such as blockchain.

1.2 Enterprise Security Challenges

The IBM LinuxONE platform provides unique capabilities to help with overcoming security challenges and differentiating your business offerings. These challenges can range from maintaining regulatory compliance so that you are not subject to fines and penalties, to ensuring that your critical systems are not compromised or taken over by malicious entities.

When you are considering an infrastructure platform, you must understand the security features that are inherent on the platform in the cloud and on-premises. IBM LinuxONE is engineering from the ground up to protect your business from all manner of cyber threats. By providing a highly securable, massively scalable, data serving platform, LinuxONE can help any business that wants to thrive in a data-centric economy.

1.2.1 Data protection and privacy

As shown in a 2019 study[2], a 29.6% chance exists that any organization will have a data breach within the next two years, with each breach costing an average of $3.92 M. A single data breach can cost your organization millions in lost customers, reduced brand equity, lost revenue, and regulatory fines.

Data protection is the practice of ensuring that data does not fall into the wrong hands, and if it does, ensuring that the data is unreadable or unusable. Encryption is the most effective way to safeguard your sensitive data from theft or misuse by unauthorized parties and is shown to reduce breach costs by an average of $360,000. Yet, of the nearly 15 billion records that were breached since 2013, only 4% were encrypted.

This lack of encryption is because until recently, encrypting data was time-consuming, expensive, and it severely degraded system performance. Businesses that chose to encrypt did it selectively, leaving the rest of their data exposed to threats.

[2] https://databreachcalculator.mybluemix.net/?cm_mc_uid=41526513840215644936275&cm_mc_sid_50200000=21830241564493627516

Four levels of data encryption deployment are available. Figure 1-1 shows that, as you move higher up in the pyramid, you gain more security control of your data at the cost of a more complex and intrusive encryption implementation. Conversely, as you go lower, complexity and costs are reduced, but with a less granular approach to encryption. Deploying data encryption on one layer or another is a tradeoff that depends on the context and regulatory environment of each client.

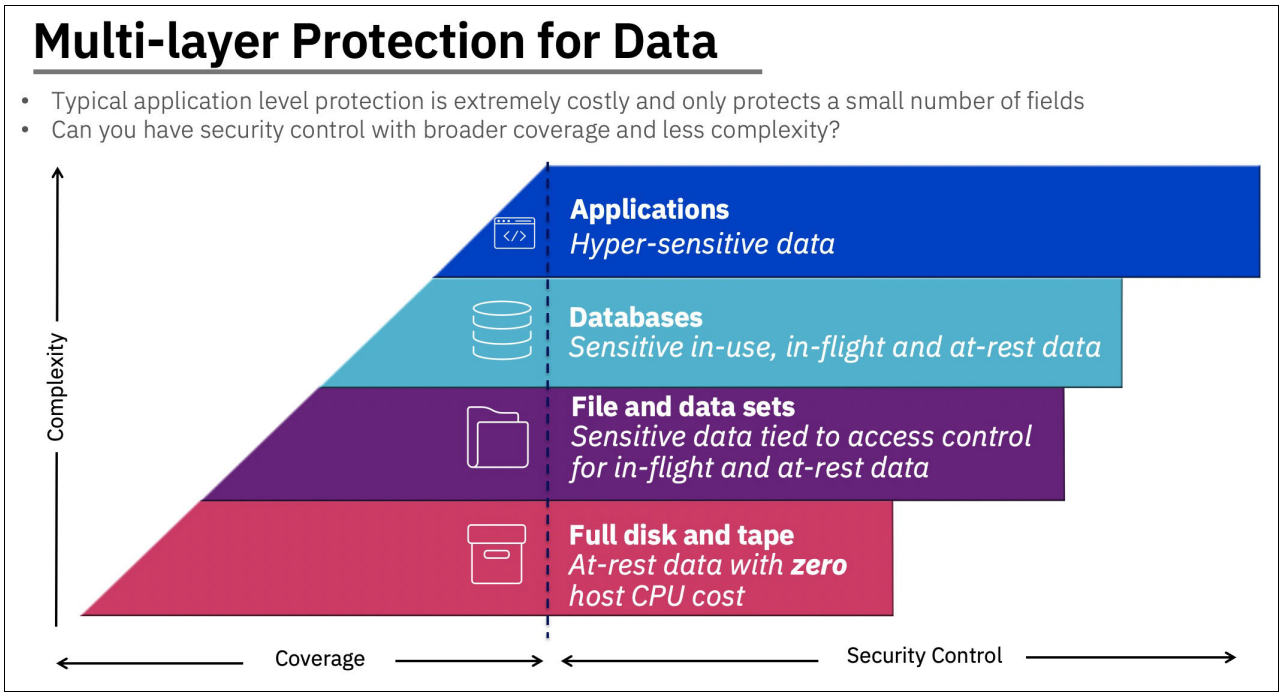


Figure 1-1 Various levels of data protection

With the latest generations of LinuxONE hardware, IBM embedded encryption logic and processing onto each processor chip in the system. This configuration allows you to encrypt massive amounts of data with little affect on your system performance.

The on-chip encryption capability is further enhanced by the IBM Crypto-Express adapter, which enables industry-leading key protection technology. This combination of integrated cryptographic hardware makes the LinuxONE platform an efficient and cost-effective solution for securely hosting various enterprise-grade Linux workloads.

For more information about these cryptographic hardware capabilities, see 2.1, “Secure cryptographic hardware” on page 16.

1.2.2 Secure hybrid cloud integration

As enterprise applications are modernized or built for cloud-native computing, it is important to ensure that these workloads and their hosting environments are secure. It is critical for users and clients to have confidence that their data is protected yet available from anywhere and on any device. The ability to be fast and flexible in delivering new services, with insight and security, is the key to differentiating a business.

IBM Secure Service Container (SSC) technology is exclusive to LinuxONE and provides an easy-to-deploy secure hosting appliance for container-based applications that run in hybrid cloud environments. SSC is a secure computing environment for microservices-based applications that can be deployed without any application code changes, which makes it an easily consumable solution for cloud-native development. It provides several unmatched security benefits, such as automatic pervasive encryption of data in-flight and at-rest, protection from privileged administrators, and tamper protection during installation and start time to protect against malware.

For more information, see 3.1, “IBM Secure Service Container” on page 32.

This service can be used as part of a private cloud deployment or through public cloud services that are hosted on IBM Cloud®. That is, a client can implement an on-premises LinuxONE machine to build a private cloud, or they can gain access to the secure services by provisioning a LinuxONE instance on the public cloud.

Running cloud services on LinuxONE allows organizations to take advantage of IBM and open-source software systems while they use container orchestration tools, such as Kubernetes in a secure cloud environment. By using automated container management tools with enterprise security capabilities, clients can securely build and host their own flexible hybrid and private cloud deployments without compromise.

For more information, see 3.3, “IBM Cloud Hyper Protect Services” on page 34.

1.2.3 Cyber resiliency and availability

In today’s digital economy, being continuously open for business is a competitive advantage. Your customers expect to transact business with you 24 x 7 with no excuses for interruptions or outages. To this end, cyber resiliency is an often overlooked method for providing business value through security. You might lose access to your core systems because of a ransom ware attack or face unplanned downtime as a result of a distributed denial of service (DDoS) attack. These types of outage can cause costly business disruptions and productivity losses.

To be competitive, enterprises must provide trusted services with high uptime to their clients, while consistently delivering new value and features. This demand from clients requires a computing platform that accommodates your developers’ creative genius and a highly secure infrastructure that provides instantaneous data delivery at any time, whether you have thousands or millions of simultaneous users.

IBM LinuxONE machines have the industry’s highest reliability levels for over a decade, with up to 99.999% or greater availability. In fact, the experts who track downtime say that the underlying hardware infrastructure is “in a class of its own.”

Engineered to help protect against insider and outsider threats in multi-tenanted cloud environments, the LinuxONE III generation introduced a new capability called the Secure Execution for Linux. It is a hardware-based security technology that is designed to protect workloads from internal and external threats to help our clients prevent security breaches. IBM Secure Execution can help protect and isolate workloads on-premises, or on IBM LinuxONE and IBM Z hybrid cloud environments. Users, and even system administrators, cannot access sensitive data in Linux-based virtual environments.

For more information, see 2.3, “IBM Secure Execution for Linux” on page 27.

The LinuxONE platform also features technology to address the next evolution in cyber attacks. The potential of quantum computing is quickly advancing, and soon will explode. This shift will force the entire industry to evolve as quantum computing might break currently secure cryptographic algorithms.

The new IBM Crypto-Express7S introduces support for quantum-safe signing algorithms to ensure that data can be secured today and well into the age of pragmatic quantum computing. The current generation of quantum-safe cryptographic algorithms were developed internally by IBM to help prevent the eventual quantum computing attacks of the future.

1.2.4 Industry and regulatory compliance

Many businesses operate on the assumption that adhering to regulatory compliance standards is enough to mitigate business risk and protect a company's data. Although this assumption might have been true in the past, it is no longer an option to implement a static compliance policy only.

Cyber threats in the modern era are constantly evolving and move too quickly for an organization to sit back with passive data protection policies. Protecting only enough data to achieve compliance should be viewed as the bare minimum, not a best practice.

Corporate risk management and compliance is an ongoing cost and effort that only increases over time. The scope of these industry and government regulations is constantly in flux. It also is expanding with more compliance requirements, and the introduction of new mandates, such as General Data Protection Regulation (GDPR).

At a high level, global security regulations feature varying requirements. However, a common thread is that most include specific requirements regarding encryption of data and access to that data. LinuxONE addresses both of these needs as a core feature of the platform.

A comparison of the how regulatory compliance is handled by LinuxONE and x86 is shown in Figure 1-2.

IBM LinuxONE capabilities	x86 capabilities
•Encrypt everything quickly and economically with hardware acceleration •Protect against side-channel attacks and insider threats with tamper resistant encrypted keys and Secure Service Containers •Isolate LPARs at the architectural level with EAL5+ design and HSM crypto isolation •Protect keys in memory with tamper resistant design (FIPS 140-2 Level 4 HSM) and encryption •Hardware-accelerated SSL/TLS encryption •Limit access to data by encrypting everything •Remove entire groups of users from audit scope •Limit access to sensitive data with Secure Service Containers (even system admins don't have access!)	•Slow/costly encryption due to lack of hardware acceleration •Vulnerable attacks due to clear keys •Weak isolation •Selectively encrypt sensitive data at best due to slow/costly encryption •Little protection against insider threat •Large audit scope

Figure 1-2 Data compliance on LinuxONE versus x86

LinuxONE provides secure hosting environments where an organization that runs on-premises or cloud-based services can ensure that their user's data is protected always. Even IT administrators with physical access to hardware cannot access data, including sensitive and personally identifiable information.

1.3 IBM LinuxONE servers

The first two LinuxONE products were named Emperor and Rockhopper. Emperor II and Rockhopper II, the second iteration of LinuxONE, were released in 2017 and early 2018. The new iteration of the system is the IBM LinuxONE III, which is available in two models: LinuxONE III LT1, which was generally available in late 2019, and LinuxONE III LT2 which was released in April 2020:

- IBM LinuxONE III LT1

  The newest member of the LinuxONE family, the IBM LinuxONE III delivers a radically new form factor, featuring a 19-inch frame that flexibly scales 1 - 4 frames. It is designed around a new 12-core, 5.2Ghz processor and is configurable with up to 190 processor cores, up to 40 TB of RAM, and 8 TB of Redundant Array of Independent Memory (RAIM) per central processing drawer.

- IBM LinuxONE III LT2

  The IBM LinuxONE III LT2 is the newest entry model into the IBM LinuxONE family of servers. It delivers a 19-inch single-frame (versus the option of up to four frames for the LT1), efficient design with a low entry cost that can easily coexist with other platforms in a cloud data center. This model is designed around a new 12-core processor chip. It is configurable with up to 65 cores running at 4.5 GHz, up to 16 TB of RAM, and 8 TB of RAIM per central processing drawer.

- IBM LinuxONE Emperor II

  This machine features up to 170 processor cores, running at 5.2 GHz, up to 32 TB of RAM, and 640 dedicated I/O processors, all housed in a dual-frame server. It supports tens of thousands of sessions and millions of containers. It can run 8,000 virtual servers and over 30 billion RESTful web interactions per day. This server is dedicated for Enterprise environments.

- IBM LinuxONE Rockhopper II

  The same technology as Emperor II, but at a lower price. It is housed in an industry-standard, 19-inch rack. Rockhopper II is available with up to 8 TB of memory and 30 processor cores, running at 4.5 GHz. It supports hundreds of production and development virtual machines (VMs) in a single footprint.

For more information, see, this web page.

1.3.1 IBM LinuxONE III LT1

The IBM LinuxONE III LT1 radically changed the footprint for LinuxONE servers. It is built with a 19-inch industry-standard frame that flexibly scales from 1 to 4 frames, depending on the configuration that is required. This new form factor maintains approximately the same maximum floor space as older generations and allows most clients to reduce their floor space significantly. The doors are designed for acoustics and optimized for air flow. The IBM LinuxONE III LT1 offers air-cooled (internal radiator) or water-cooled systems (WCS).

At the heart of the LinuxONE III LT1 is the new processor chip, made with 12 cores and leveraging the density and efficiency of 14 nm silicon-on-insulator technology, Running at 5.2Ghz, it delivers increased performance and capacity across a wide range of workloads.

Up to 190 client configurable cores are available (known as IFLs, or Integrated Facility for Linux). The IBM LinuxONE III LT1 includes processor capacity that is represented by feature codes.

Five processor capacity feature codes are available for the IBM LinuxONE III: Max34, Max71, Mac108, Max145, and Max190. The numbering signifies that, for example, a Max 34 can configure up to 34 IFLs (cores), Max71 for up to 71 IFLs, and so on.

The system offers 8 TB of Redundant Array of Independent Memory (RAIM) per central processing complex (CPC) drawer and up to 40 TB per system. RAIM is intended to provide redundancy for primary memory, sockets, and memory channels for more reliability and availability.

IBM Virtual Flash Memory (VFM) is now in the RAIM and provides high levels of availability and performance. IBM Adapter for NVMe supports the Non-Volatile Memory express (NVMe) communications protocol, which was built specifically for solid-state drives (SSDs). This feature brings integrated storage to LinuxONE by allowing a client-procured SSD up to 64 TB to be directly connected to the I/O subsystem through an IBM PCIe adapter. It provides the low latency and high I/O throughput that can help with real-time analytics, memory-intensive and fast storage workloads (such as streaming and paging/sorting), and traditional applications, such as relational databases.

IBM LinuxONE III LT1 also integrates new hardware compression capabilities, which delivers greater compression throughput than previous generation systems. This on-chip compression co-processor uses industry standard compression algorithms and can reduce data storage requirements and costs. This compression can also increase data transfer rates to boost throughput above comparable x86 CPUs; all without adversely impacting response times.

For more information about the IBM LinuxONE III, see this web page.

LinuxONE III LT1 data sheet

The data sheet for LinuxONE III LT1 model is shown in Table 1-1.

Table 1-1 LinuxONE IIII LT1 at a glance

IBM LinuxONE III LT1 features		
LinuxONE III Models	**Cores**	**Memory: Min - Max**
LT1	Up to 190	512 GB - 40 TB
Cryptography		
Crypto-Express7S	Minimum 2 features; maximum 30 features	
Disk Connectivity		
Next generation IBM FICON® Express16SA	Maximum: 192 features	
FCP Express32S	Maximum: 192 features	
IBM Adapter for NVMe1.1	Maximum: 16 features	
Connectivity		
HiperSockets	Up to 32 high-speed virtual local area networks	

IBM LinuxONE III LT1 features	
Shared Memory Communications - Direct Memory Access (SMC-D)	Up to 32 ISM virtual CHIPDs
Supported Linux distributors	
Red Hat	Red Hat Enterprise Linux (RHEL 6.10, RHEL 7.7 and 8.0)
SUSE	SUSE Linux Enterprise Server (SLES) 12 SP4 and 15SP1
Canonical	Ubuntu 18.04 and Ubuntu 16.04
Supported hypervisors	
IBM z/VM	z/VM V7.1, z/VM 6.4
KVM	KVM hypervisor, which is offered with the following Linux distributions: RHEL 7.6 or higher, SLES-12 SP2 or higher, Ubuntu 18.04 or higher
IBM partitioning technology	Up to 85 LPARs for secure workload isolation

1.3.2 IBM LinuxONE III LT2

The LinuxONE III is an air-cooled, single frame, efficient design, with a low entry cost. As with the other servers in the LinuxONE family, it is designed to help enable cloud native development and deployment, achieve encryption everywhere, and provide cyber resiliency to ensure scalable isolation of workloads to protect from threats, while ensuring continuous availability of services. The system offers up to 40 LPARs, allowing for various workloads to run on a single server.

The LinuxONE III LT2 is based on the 12-core processor chip that leverages the density and efficiency of 14 nm silicon-on-insulator technology. This model LT2 is available with five feature-based sizing options: Max4, Max13, Max21, Max31, and Max65. The LinuxONE III LT2 design incorporates two Central Processor Complex (CPC) drawers for the Max65. The numbering signifies that, for example, a Max21 can configure up to 21 IFLs (cores), Max31 for up to 31 IFLs, and so on. The cores run at 4.5Ghz.

The system offers 8 TB of Redundant Array of Independent Memory (RAIM) per CPC drawer and up to 16 TB total per LinuxONE III LT2 system, depending on the configuration. RAIM is intended to provide redundancy for primary memory, sockets, and memory channels for added reliability and availability. IBM Virtual Flash Memory (VFM) is now in the RAIM and provides high levels of availability and performance.

As with the LinuxONE III LT1, the LT2 model also brings an integrated storage option to LinuxONE by supporting carrier cards into which NVMe SSDs can be plugged. It provides the low latency and high I/O throughput that can help with real-time analytics, memory-intensive and fast storage workloads, such as streaming, paging and sorting, and traditional applications, such as relational databases.

An Integrated Accelerator is available for zEDC on the LinuxONE III LT2 processor chip. Clients no longer need to purchase zEDC Express adapters for their servers. The Integrated Accelerator for zEDC provides values for existing and new compression users along with less CPU consumption for compression.

Pervasive usage that is enabled in highly virtualized environments gives all LPARS and virtual machines 100% access. Therefore, customers no longer must choose which Linux guests can use the accelerator and applications for compression.

LinuxONE III LT2 data sheet

The data sheet for LinuxONE III LT2 model is shown in Table 1-2.

Table 1-2 LinuxONE IIII LT2 at a glance

IBM LinuxONE III LT2 features		
LinuxONE III Models	**Cores**	**Memory: Min - Max**
LT2	Up to 65	64 GB - 16 TB
Cryptography		
Crypto-Express7S	Minimum 2 features; maximum 30 features	
Disk Connectivity		
IBM FICON Express16S+	Maximum: 192 features	
FCP Express32S	Maximum: 192 features	
IBM Adapter for NVMe1.1	Maximum: 16 features	
Connectivity		
HiperSockets	Up to 32 high-speed virtual local area networks	
Shared Memory Communications - Direct Memory Access (SMC-D)	Up to 32 ISM virtual CHIPDs	
Supported Linux distributors		
Red Hat	Red Hat Enterprise Linux (RHEL 6.10, RHEL 7.7, and 8.0)	
SUSE	SUSE Linux Enterprise Server (SLES) 12 SP4 and 15SP1	
Canonical	Ubuntu 18.04 and Ubuntu 16.04	
Supported hypervisors		
IBM z/VM	z/VM V7.1, z/VM 6.4	
KVM	KVM hypervisor, which is offered with the following Linux distributions: RHEL 7.6 or higher, SLES-12 SP2 or higher, Ubuntu 18.04 or higher	
IBM partitioning technology	Up to 40 LPARs for secure workload isolation	

1.3.3 IBM LinuxONE Emperor II

Emperor II is available with up to 170 configurable cores that use a 5.2 Ghz processor for unmatched performance and massive scaling.

The vertical scale allows Emperor II to scale up to 2 million Docker containers in a single system. It can serve up to 30 billion web data requests a day and can host databases that are 20 times larger, without the added cost and latency of fragmenting data across server farms. Another 640 processors are dedicated to I/O processing to increase I/O speeds and assure data integrity.

With 32 TB of real memory, Emperor II can open opportunities, such as in-memory data marts, large buffer pools for data access, and in-memory analytics. Advances in the machine instruction set of the processor help to accelerate analytic workloads by using the Vector Packed Decimal Facility, which allows packed decimal operations to be performed in registers rather than memory.

Java improvements, such as pause-less garbage collection, enables vertical scaling. The use of crypto-acceleration delivers more improvements in throughput per core, which provides a boost to Java processes that use cryptographic functions.

For more information about the IBM LinuxONE Emperor II, see this web page.

LinuxONE Emperor II data sheet

The data sheet for Emperor II models is shown in Table 1-3.

Table 1-3 IBM LinuxONE Emperor II at a glance

IBM LinuxONE Emperor II features		
Emperor II Models	**Cores: Min - Max**	**Memory: Min - Max**
LM1	1 - 33	256 GB - 8 TB
LM2	1 - 69	256 GB - 16 TB
LM3	1 - 105	256 GB - 24 TB
LM4	1 - 141	256 GB - 32 TB
LM5	1 - 170	256 GB - 32 TB
Cryptography		
Crypto-Express6S	Minimum 2 features; maximum 16 features	
Crypto-Express5S	Minimum 2 features; maximum 16 features	
Disk Connectivity		
FICON Express16S+/FICON Express16S/FICON Express8	Maximum: 320 ports	
NIC - Connectivity		
10 GbE RoCE Express2	Maximum 8; minimum recommended: 2	
OSA - Express6S	Maximum: 96 ports	
OSA - Express5S	Maximum: 96 ports	
High-speed “Virtual” LANS		
HiperSockets	Up to 32 connections	
Supported Linux distributors		
Red Hat	Red Hat Enterprise Linux (RHEL) 6 and 7	
SUSE	SUSE Linux Enterprise Server (SLES) 11 SP4, SLES 12 SP2, and SLES 15	
Canonical	Ubuntu 16.04 LTS and Ubuntu 18.04 LTS	
Supported hypervisors		
IBM z/VM	z/VM 6.4 (until the EOS) and z/VM 7.1 or higher	

IBM LinuxONE Emperor II features		
KVM	KVM hypervisor, which is offered with the following Linux distributions: SLES-12 SP2 or higher, Ubuntu 16.04 or higher, and RHEL 7.5 or higher	
IBM partitioning technology	Up to 85 LPARs for secure workload isolation	
Typical physical weight of air-cooled configuration	**Minimum configuration weight of new build LM1**	**Maximum configuration weight of new build LM5**
With Internal Battery Feature (IBF)	LM1 1461 kg (3219 lb.) with overhead cabling 1531 kg (3375 lb.)	LM5 2705 kg (5961 lb.) with overhead cabling 2775 kg (6117 lb.)
Without Internal Battery Feature (IBF)	LM1 1258 kg (2772 lb.) With overhead cabling 1328 kg (2928 lb.)	LM5 2400 kg (5290 lb.) With overhead cabling 2471 kg (5446 lb.)
Product Dimensions (D x W x H) without overhead cabling	186.7 x 156.5 x 201.3 cm (73.5 x 61.6 x 79.3 in)	
Product Dimensions (D x W x H) with overhead cabling	186.7 x 184.7 x 215.3 cm (73.5 x 72.7 x 84.8 in)	
Airflow (Capacity of Exhaust)	6370 cubic meters per hour (3800 CFM)	

1.3.4 IBM LinuxONE Rockhopper II

Rockhopper II delivers secure capabilities in a 19-inch frame with a lower cost of entry that can coexist with other platforms in any cloud data center. It is built on the strong foundation of the LinuxONE Emperor II platform.

Rockhopper II is housed in an industry-standard, 19-inch IBM-supplied rack. The design includes power distribution unit (PDU)-based power and redundant power, cooling, and power cords. These features allow you to install Rockhopper II within any data center with a server that is rated at ASHRAE A3. Up to 16U of available frame space can be used in the new 19-inch rack design.

For more information about the IBM LinuxONE Rockhopper II, see this web page.

LinuxONE Rockhopper II data sheet

Table 1-4 provides some basic information about Rockhopper II models.

Table 1-4 IBM LinuxONE Rockhopper II at-a-glance

IBM LinuxONE Rockhopper II features		
Rockhopper II models	**Cores: Min - Max**	**Memory: Min - Max**
LR1 Max4	1 - 4	64 GB - 2 TB
LR2 Max12	1 - 12	64 GB - 4 TB
LR3 Max24	1 - 24	64 GB - 8 TB
LR4 Max30	1 - 30	64 GB - 8 TB
Cryptography		

IBM LinuxONE Rockhopper II features		
Crypto-Express6S/Crypto Express5S	Minimum 2 features; maximum 16 features	
Disk connectivity		
FICON Express16S+/FICON Express16S / FICON Express8S	Maximum features (two ports per feature)	
Max4	16	
Max12	32	
Max24, Max30	64	
NIC - Connectivity		
10 GbE RoCE Express2, 10 GbE RoCE Express	4 Maximum features (two ports per feature); minimum recommended is 2	
OSA-Express6S / OSA-Express5S / OSA-Express4S / 1000-BaseT	Maximum features (two ports per feature)	
Max4	16	
Max12	32	
Max24, Max30	48	
High Speed “Virtual” LANs		
HiperSockets	Up to 32 high-speed “virtual” local area networks	
Supported Linux distributors		
Red Hat	Red Hat Enterprise Linux (RHEL) 6 and 7	
SUSE	SUSE Linux Enterprise Server (SLES) 11 SP4, SLES 12 SP2, and SLES 15	
Canonical	Ubuntu 16.04 LTS and Ubuntu 18.04 LTS	
Supported Hypervisors		
IBM z/VM	z/VM 6.4 (until the EOS) and z/VM 7.1 or higher	
KVM	KVM hypervisor, which is offered with the following Linux distributions: SLES-12 SP2 or higher, Ubuntu 16.04 or higher, and RHEL 7.5 or higher	
IBM partitioning technology	Up to 40 LPARs for secure workload isolation	
Typical Physical Weight	Minimum configuration weight of new build 735 kg (1621 lb) Maximum configuration weight of new build 795 kg (1753 lb)	
Weight without side covers	Without overhead cabling 735 kg (1621 lb.)	With overhead cabling adds approximately 12 lb. (5 kg) 1633 lbs. (740 kg)
Weight with side covers adds approximately 42.7 lbs. (19.4 kg)	Without overhead cabling 754 kg (1663 lb.)	With overhead cabling adds approximately <12 lbs. (5 kg) 1675 lbs. (760 kg)

IBM LinuxONE Rockhopper II features		
	Note: Optional seismic resistance hardware adds approximately 35 kg (78 lb.)	
Product Dimensions (D x W x H) without side covers	Without overhead cabling: 107 x 60 x 201.5 cm (42.1 x 23.6 x 79.3 in)	With overhead cabling increases height 107 x 60 x 212.3 cm (4.3 inches 42.1 x 23.6 x 83.6 in)
Product Dimensions (D x W x H) with side covers	Without overhead cabling 120.4 x 62.4 x 202 cm (47.4 x 24.6 x 79.5 in)	With overhead cabling increases height 120.4 x 62.4 x 212.8 cm (47.4 x 24.6 x 83.8 in)
Airflow (Capacity of Exhaust)	2000 cubic meters per hour (1200 CFM)	

2

Core security technologies on LinuxONE

In the era of ever-present attacks and breaches, security and compliance regulations became very important.

A secure digital business starts at the hardware level. LinuxONE helps you to establish foundational system integrity across physical and virtual infrastructure to address rapidly evolving security threats to your enterprise.

LinuxOne is a secure platform. The LinuxONE Infrastructure Platform includes security features that are embedded in the platform for workloads in the cloud and on-premises.

In this chapter, we cover the core technologies that are embedded in the LinuxONE hardware for ensuring a pervasive level of data secure protection.

This chapter includes the following topics:

2.1 Secure cryptographic hardware

Traditionally, encryption of all your data requires a large amount of time and computation overhead. This need is the result of the limitations of software-based encryption, which shares computing resources with the rest of your system, and can slow down other shared applications.

Although it can be cheap to get started with software-based encryption, it quickly becomes prohibitively expensive as you scale your business. Especially with more secure forms of encryption (more complex algorithms, longer bit values), it becomes resource-intensive. Therefore, you typically must pay more for extra processing power for the same level of performance.

The LinuxONE solution to this problem is through dedicated hardware that is tuned for encryption and can encrypt 100% of data that is at-rest and in-flight (by default) with minimal compute overhead. The security is embedded in every feature of the hardware and software stack. This level of protection is achieved by using hardware accelerated encryption capabilities and does not require any code or application changes.

The LinuxONE solution provides improved trust and reduced risk through hardware encryption that is fast and strong enough to encrypt all data it manages, with designed-in redundancy to deliver a highly available single point of truth.

LinuxONE allows for secure platform simplification by providing the following benefits:

- Protecting all applications and fully encrypting their data without any changes to the business applications, including built-in hardware acceleration that allows for faster encryption.
- Enabling bulk encryption that is simple, transparent, and features optimized performance to secure your cloud infrastructure.

Types of cryptographic keys

An important starting point for understanding the cryptographic hardware on LinuxONE is the types of encryption keys that are used. LinuxONE cryptography uses the types of encryption keys that are listed in Table 2-1.[1]

Table 2-1 Encryption key types for LinuxONE

Key type	Description
Data	A data-encrypting key that is used to encrypt and decrypt data.
Key-encrypting	A key that encrypts or wraps other keys.
Effective	A type of data-encrypting key; also called a *data key* that is wrapped by a key-encrypting key (KEK).
Master	A special KEK that is in a tamper-responding, Crypto Express adapter only and sits at the top of a KEK hierarchy. Loading and managing the master key can be done by using the Trusted Key Entry (TKE) workstation.
CPACF wrapping	A special key-encrypting key that is generated at LPAR activation and is in the Hardware System Area, which is inaccessible to applications and the operating systems. It is used to create protected keys.

[1] https://www.ibm.com/support/knowledgecenter/en/linuxonibm/com.ibm.linux.z.lxdc/lxdc_terminology.html

Key type	Description
Secure	Key values are encrypted under a Master Key and no key ever appears in decrypted form outside of the Crypto Express HSM. Crypto operations are performed only within the Crypto Express HSM.
Clear or plain	A data-encrypting key that is not encrypted by any other key. The key material is in plain text.
Protected	Key values are encrypted under a CPACF wrapping key. Crypto operations are performed by using only CPACF. When the key is not in use, it is protected by the Crypto Express HSM. In the case of Linux in a native LPAR, the wrapping key is specific to the LPAR. However, for guests of z/VM or KVM, the wrapping key is specific to the guest.
Operational	A key that is not a master key or KEK, such as a data-encrypting key (which can be clear, secure, or protected).

The tradeoff between clear key, protected key, and secure key encryption implementations are shown in Figure 2-1.

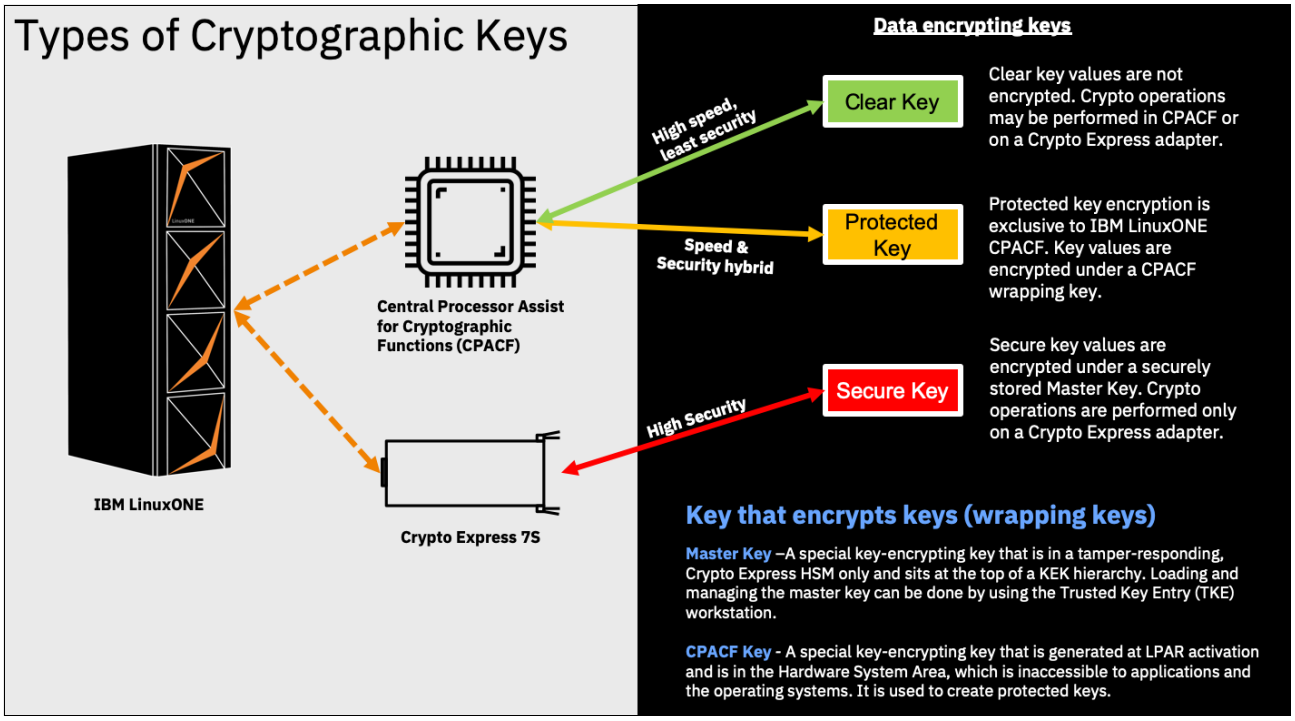


Figure 2-1 Encryption key implementations and tradeoff

Cryptographic key management

Cryptographic key management is a complex task that must be managed according to strict policies. You must account for various legal, regulatory, and compliance requirements. Your key management system should allow authorized persons a method for key identification, exchange, separation, update, backup, and management.

For more information about key management, see “Cryptographic Key Management for LinuxONE” on page 36

2.1.1 Central Processor Assist for Cryptographic Functions

The hardware accelerated encryption capabilities of LinuxONE are enabled by Central Processor Assist for Cryptographic Functions technology (CPACF). The CPACF on-chip encryption co-processor is on every compute chip that is next to the main processor and can encrypt up to 13 GB of data per second per core. This configuration results in performance improvements of up to 6x and is best suited for symmetric, high-speed bulk encryption.

CPACF supports the AES, DES, TDES, SHA-1, SHA-2, SHA-3, and Elliptic Curve Cryptography (ECC) algorithms. ECC support on CPACF for LinuxONE III is something new that helps accelerate applications, such as IBM Blockchain Platform. In these cases, the application code does not need to be changed, but it still can take advantage of better performance and acceleration throughput of ECC functions, such as EdDSA (Ed448, Ed25519), ECDSA (P-256, P-384, P-521), and ECDH.

CPACF is a no-charge feature of LinuxONE. If you have the hardware, you can enable the technology and start to get the benefits right away.

True Random Number Generator

Another feature of LinuxONE cryptographic hardware is the ability to generate unreproducible, unique data with the on-chip true random number generator (TRNG). This capability is the basis for generating high-quality cryptographic keys. TRNG is an improvement of Deterministic RNG because the numbers that are generated are more random.

Protected key encryption

The ability to use protected key encryption with CPACF is a differentiating feature on LinuxONE. Many encryption services use plaintext “clear keys” that are stored unsecured in main system memory. These clear keys are visible and vulnerable during the encryption and decryption process. Clear keys can be stolen from memory or system dumps, meaning that your encrypted data is now at risk.

Protected key technology uses CPACF for encrypting data at high speeds without exposing keys to main system memory. The data-encrypting (protected) keys are encrypted or “wrapped” by a special key that is stored in a secure environment. In that environment, it is inaccessible to applications, hypervisor, and operating system (known as the HSA, or Hardware System Area). Among the many use cases, this technology enables fast and highly secure encryption and decryption of complete disks (volumes) or selected partitions.

With the introduction of LinuxONE III, CPACF supports the creation of protected key signatures.

2.1.2 IBM Crypto Express adapter

LinuxONE can also include IBM Crypto Express adapters, a Hardware Security Module (HSM), and a cryptographic co-processor that supports high-speed, asymmetric encryption. This co-processor also supports a symmetric cryptographic function to assist key encryptions, encrypt data, compute message authentication codes, protect financial PINs, secure EMV card transactions, and many other functions. This specialized hardware performs AES, DES, TDES, RSA, ECC, SHA-1, SHA-2, SHA-3, and other cryptographic operations.[2]

[2] https://www.ibm.com/support/knowledgecenter/en/linuxonibm/com.ibm.linux.z.wskc.doc/wskc_c_ch1ccafuncover.html

An HSM is designed to withstand physical and logical attacks and features special hardware to perform cryptographic operations and protect keys. The HSM is accessed from a host computer that uses a set of generic or specialized API functions. The IBM Crypto Express HSM can support the following primary secure key cryptographic modes, APIs, and one clear key accelerator mode. You also can reload your HSM firmware at any time to switch from one to the other:

- IBM Common Cryptographic Architecture (CCA)

  CCA provides a set of general-purpose cryptographic functions. Its primary strength is support of finance industry payments applications. This mode is also often called *cryptographic co-processor mode*, and many IBM software products support CCA modes to enhance security.

- IBM Enterprise PKCS #11 (EP11) mode.

  This mode supports the industry standard PKCS #11 API. EP11 is designed for customers who seek support for open standards and enhanced security. It offers a various general purpose, secure-key-only cryptography functions.

- Accelerator

  This mode makes Crypto Express hardware become an asymmetric cryptographic function accelerator. When tested with a Crypto Express 6S running on LinuxONE as an accelerator mode with eight concurrent processes, it can process approximately 9 K SSL/TLS handshakes per second with 2048-bit RSA key.[3] This mode might be useful for enterprise web services.

Figure 2-2 shows new Crypto Express Adapter options for LinuxONE III with enhanced performance and throughput, and support for new cryptographic algorithms.

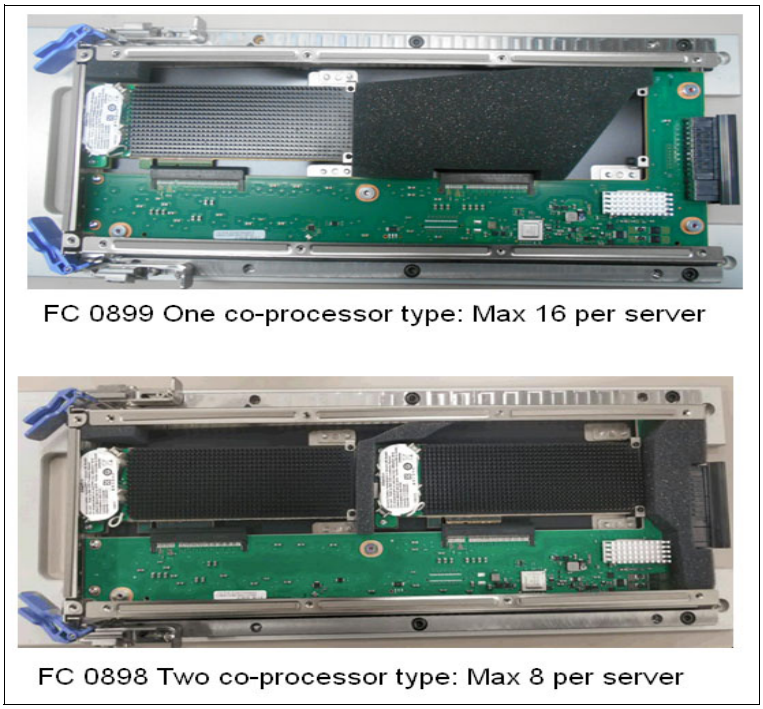


Figure 2-2 Two options for Crypto Express Cards for LinuxONE III

For more information about these cryptographic devices, see this web page.

[3] https://www.ibm.com/security/cryptocards/pciecc3/performance

HSM Certifications

The IBM Crypto Express adapter is a Hardware Security Module that is certified for FIPS 140-2 Level 4. This certification applies to all adapter modes. This means the cryptographic co-processors are protected within a tamper-resistant and tamper-responsive environment that erases encryption keys if it senses an attack, eliminating the risk of exposing cryptographic keys during a breach.

The IBM Crypto Express adapter is also certified for PCI-HSM, which applies to the Common Cryptographic Architecture (CCA) firmware / cryptographic coprocessor mode. Common criteria applies to the EP11 firmware coprocessor mode.

The following section describes how the Crypto Express adapter HSM can provide the maximum protection for your encryption keys.

FIPS certification levels

The Federal Information Processing Standard (FIPS) Publication 140-2 (FIPS PUB 140-2), is a US government computer security standard that is used to approve cryptographic modules. It defines what areas of security requirement to meet the standard in terms of design and behaviors of the module. These requirements include specification, ports and interfaces, roles and services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

For more information about the FIPS 140-2 standards, see the US Department of Commerce's federal information processing standards publication *Security Requirements for Cryptographic Modules*.

Figure 2-3 on page 21 shows a summary of the following levels of FIPS 140-2 that it is certified to protect against. You can see that the level 4 device meets the highest requirements, and IBM Crypto Express adapter for LinuxONE is designed to meet those level 4 requirements:

- Level 1: No physical security features required.
- Level 2: Tamper-evident physical security features.
- Level 3: Tamper-responding features designed to notify of unauthorized access.
- Level 4: Complete tamper-responding envelope of protection that immediately deletes all plaintext keys upon detection of unauthorized access.

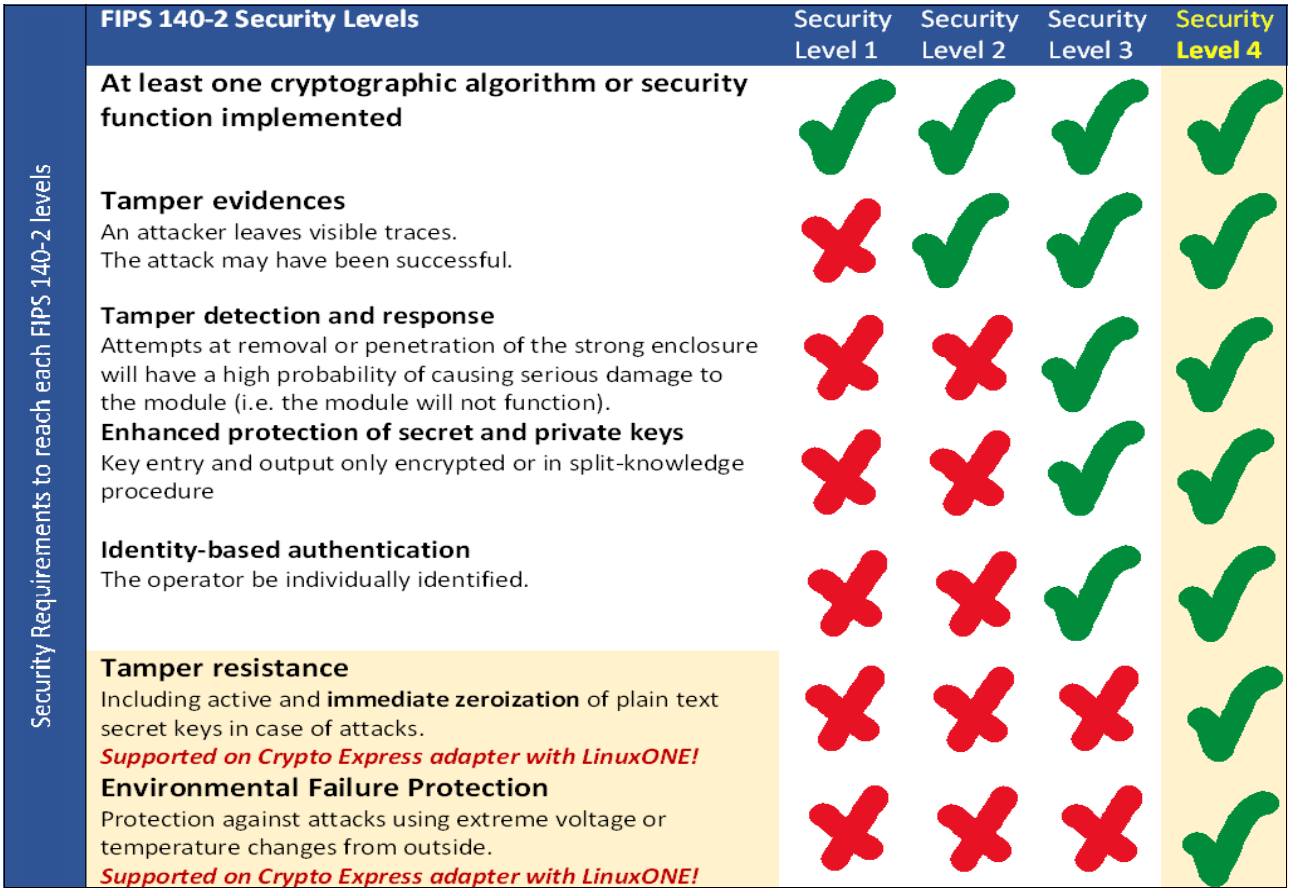


Figure 2-3 Different certification levels of the FIPS 140-2 Standard

Secure key encryption

The HSM feature of the IBM Crypto Express adapter enables secure encryption with the capability to protect cryptographic keys that use a special key called Master Key. (We use the terms *HSM* and *Crypto Express adapter* interchangeably in this document.)

The master key is used to encrypt the keys that are used by your applications, which are stored outside of the Crypto Express HSM. Those keys are fully protected because the Master Key is protected by the security features of the HSM.

The Master Key is stored in Crypto Express adapter hardware. Loading and managing the Master Key into the Crypto Express adapter can be done in software, but it is highly recommended to perform it with the Trusted Key Entry (TKE) workstation. For more information about TKE and key management, see Chapter 3, “Users of security on LinuxONE” on page 31 and Chapter 4, “Use cases” on page 43.

Secure key encryption uses a wrapped key for encrypting data that never appears in clear text outside of a secure environment. The Cypto Express adapter ensures that these keys are never exposed in the clear. Any unauthorized attempts to access the Crypto Express adapter enclosure result in the deletion of the stored keys.

Figure 2-4 on page 22 shows a high-level workflow of how master keys and secure keys are used in LinuxONE. Four different types of Master Keys for Crypto Express Adapter are available: AES, DES, RSA, and ECC. For each Master Key type, the adapter can set up to 85 domains, which is designed to support up to 85 LPARs in LinuxONE II and III system.

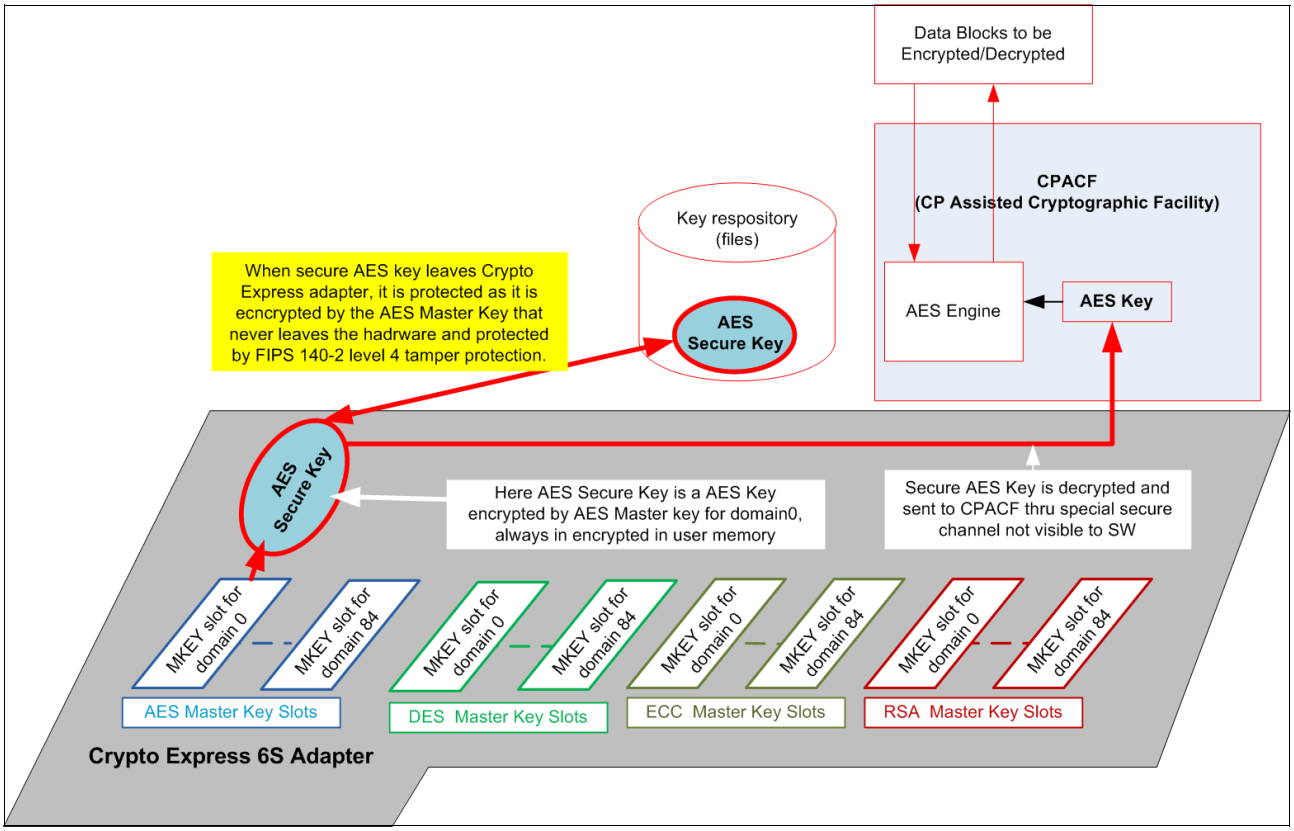


Figure 2-4 Master Keys and Secure Keys with Crypto EXpress adapter for LinuxONE

Creating a secure key

At the time of this writing, the Crypto Express for LinuxONE supports AES encryption for the user-defined secure key. The hardware is designed to support RSA, DES, AES, and ECC to be the secure keys. For more information about updates, regularly visit IBM Knowledge Center.

Figure 2-5 shows an example of a secure key use case, which is a high-level process that is used to create a secure key for an LUKS2 format volume to encrypt a disk volume by using a secure key and protected key.

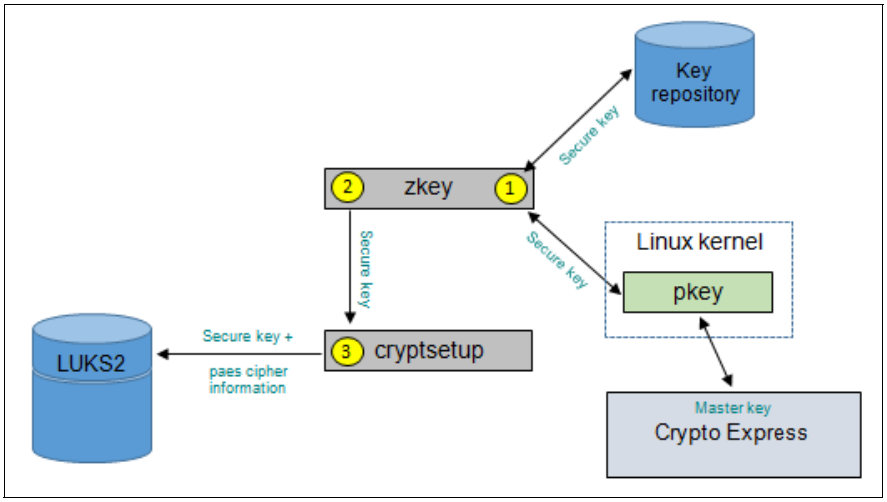


Figure 2-5 Creating a secure key

This process includes the following steps:

1. A secure key is created by using a **zkey** command. The **zkey** utility generates the secure key with the help of the **pkey** utility and an assigned Crypto Express adapter (with master key). The secure key is also stored in the key repository.
2. The use of the **zkey cryptsetup** command generates output strings that are copied and pasted to the **cryptsetup** command to create the encrypted volume with the appropriate secure key.
3. The **cryptsetup** utility formats the physical volume and writes the encrypted secure key.

An example of this process is shown in Figure 4-1 on page 45. For more information, see *Getting Started with Linux on Z Encryption for Data At-Rest*, SG24-8436.

2.2 Virtualization technology

Modern data serving systems must scale up and scale out in size, performance, and features immediately. Virtualization, which is essentially the creation of a virtual version of a computing system with a subset of total resources, is a key technology that enables any hardware system to achieve this level of scaling performance.

Thankfully, virtualization is one of the core strengths of the LinuxONE platform. The LinuxONE platform is virtualized, with the goal of maximizing utilization of computing resources. Is also lowers the overall cost and resource requirements for running critical workloads for enterprises.

The embedded architecture and hardware on LinuxONE is thoughtfully designed around the ability to partition resources (compute, memory, storage, and network) to be used independently in distinct virtualized environments.

Virtual machine

A virtual machine (VM) is a virtual environment that provides the core functionality of a single physical computer. It typically runs its own operating system and uses a fraction of the host server's total compute, memory, storage, and network resources. VMs are sometimes referred to as *guests* or *images*. As the name indicates, LinuxONE can host many distributions of Linux as guests, including Red Hat, SUSE, and Ubuntu.

Hypervisor

The hypervisor is a core part of the virtualization technology stack (see Figure 2-6 on page 24). Hypervisors are designed to enable simultaneous execution of multiple operating systems and allocating the correct amount of virtual resources. The hypervisor is necessary to run and manage other virtual machines guests. LinuxONE supports three key virtualization technologies: z/VM, KVM, and PR/SM. Each virtualization technology has its own strengths and benefits to the enterprise applications. These hypervisors are described in the next section.

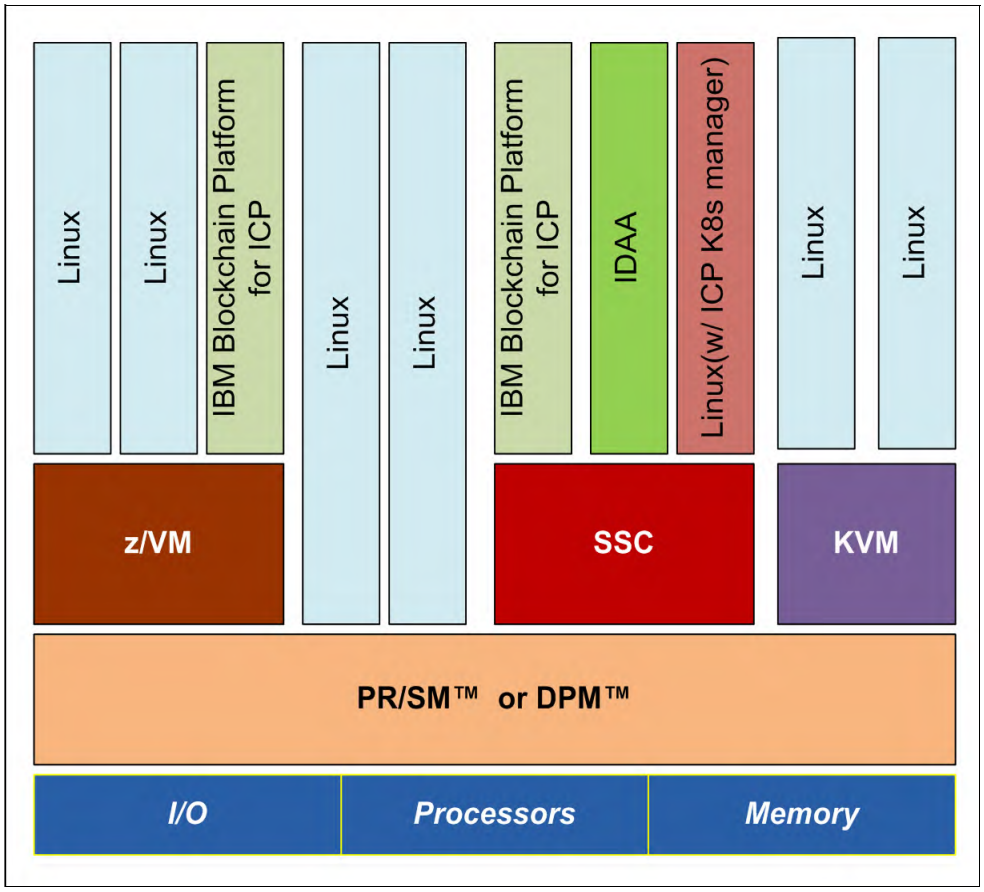


Figure 2-6 Hypervisors and virtualization technology on LinuxONE

2.2.1 PR/SM and LPARs

The IBM LinuxONE system has a unique capability to implement a hypervisor at the hardware and firmware level. The hardware hypervisor is IBM Processor Resource/Systems Manager (PR/SM), which is informally referred to as PRISM. PR/SM is implemented in firmware as a part of the base system that fully virtualizes the system resources and runs without any extra software.

PR/SM is a Type-1 hypervisor that runs directly on bare metal. With it, you create multiple isolated partitioned environments on the same physical server. These isolated environments are known as *logical partitions* (LPARs).

EAL 5+ isolation and cryptographic key protection

LinuxONE systems feature EAL 5+ isolation and cryptographic key protection[4]. EAL5+ is a regulatory certification for LPARs that verifies the separation of partitions to improve security. Therefore, you can run many virtual servers concurrently, and use LinuxONE's ability to isolate and protect each virtual server as though they were running on physically separated servers.

LinuxONE LPARs provide excellent isolation between each other, but not between the VMs or containers within the same LPAR. Secure Execution for Linux is a LinuxONE III hardware capability that hypervisors can use to isolate virtual machines and containers from each other within an LPAR

[4] https://www.commoncriteriaportal.org/files/epfiles/0900a_pdf.pdf

LinuxONE's PR/SM-based LPARs are the only technology that is commercially available that can provide this highly certified level of isolation between workloads.

Isolation and cryptographic key protection is achieved by using a dedicated cryptographic coprocessor. The CP Assist for Cryptographic Function (CPACF) delivers cryptographic and hashing capabilities in support of clear-key operations. The Crypto Express adapter is used to create the fortified data perimeter by using the IBM LinuxONE protected key in which the keys that are used in the encryption process are not visible to the applications and operating system.

Each LPAR on a LinuxONE system has its own uniquely generated and assigned cryptographic keys that are held in a secure hardware area. This configuration provides a level of cryptographic isolation between secure environments that is called for under many regulatory compliance frameworks (for example, PCI-DSS).

2.2.2 Kernel-based virtual machine

Kernel-based virtual machine (KVM) is the most popular open source Linux hypervisor and a key technology for the LinuxONE platform. It is a Type-2 hypervisor that provides simple, cost-effective virtualization technology for Linux workloads. It also allows sharing of CPU, memory, and I/O resources and can coexist with other types of virtualization technologies simultaneously running on LinuxONE. KVM on LinuxONE frees operators to adopt and switch from various hardware platforms, and more familiar interfaces.

For more information about use cases and examples, see this web page.

One of the advantages for KVM virtualization is the familiar standard Linux user interfaces for open source developers, offering a low barrier to adoption and easy integration with hybrid environments.

KVM on LinuxONE is supported through the following Linux distribution partners:

- Red Hat Enterprise Linux (RHEL)
- SuSE Linux Enterprise Server (SLES)
- Canonical Ubuntu

2.2.3 z/VM

IBM z/VM provides high levels of extreme security, scalability, and efficiency; therefore, it also provides a robust foundation for on-premises cloud computing. The z/VM virtualization technology is designed to run hundreds to thousands of Linux servers on a single IBM Z or IBM LinuxONE server with the highest degrees of efficiency, elasticity, and security. Its ability to support numerous machine images and solution's architectures provides a highly flexible production and test environment for IBM Z and LinuxONE operating systems

Do more with less. Virtualization helps to deploy more servers, networks, applications, and data on less physical hardware, and the capacity of Z/LinuxONE is outstanding. With LinuxONE, you can achieve nearly 100% utilization of system resources nearly 100% of the time. Virtualization on LinuxONE provides high levels of resource sharing, I/O bandwidth, and system availability.

Consider the following points:

- You can reduce costs on a bigger scale by running software that is paid by core on fewer cores, which saves on software license fees.
- High server density helps to use less power and floor space.

- The high resiliency of z/LinuxONE minimizes hardware that is needed for business continuance and disaster recovery.

Manage growth and complexity in the following ways:

- In support of the high density and mass of virtual servers, facilities for lifecycle management are provided (for example, workload management, monitoring, security, charge back, patching, backup, and recovery).
- Hardware resources can be added to a running system without disruption, which helps on a continuous business operation and availability of the services.
- LinuxONE can scale horizontally and vertically, scaling workload deployment on such a “scale up” machine means fewer components to manage.

Provide more flexibility and minimize lead time for new projects by using:

- Workload deployment to a single IBM Z or IBM LinuxONE server offers significant advantages in terms of flexibility.
- Rapid provisioning, which reduces lead time for new IT projects and helps to increase business agility.
- Resources that can be assigned dynamically and efficiently between workloads, whenever and wherever they are needed.
- Virtual machines for Cloud deployment. IBM Cloud Paks are based on Red Hat OpenShift Container Platform; OCP 4.2 needs z/VM-based VMs for the implementation

z/VM is IBM’s internally developed Type-2 hypervisor that manages the sharing of a LinuxONE system’s physical resources between virtual guests. The z/VM hypervisor typically runs on an LPAR and manages Linux VMs. It also can manage other types of operating systems, including z/VM, on top of the hypervisor.

z/VM is a proven and established virtualization platform with industry-leading capabilities for efficient vertical and horizontal scaling that was proven over many decades. For more information, see this web page.

The following operating systems are supported:

- Red Hat Enterprise Linux 8, Red Hat Enterprise Linux 7, Red Hat Enterprise Linux 6, and Red Hat Enterprise Linux 5
- SUSE Linux Enterprise Server 15, SUSE Linux Enterprise Server 12, SUSE Linux Enterprise Server 11, and SUSE Linux Enterprise Server 10
- Ubuntu 18.04 and Ubuntu 16.04

The smart economics of the use of z/VM are shown in Figure 2-7.

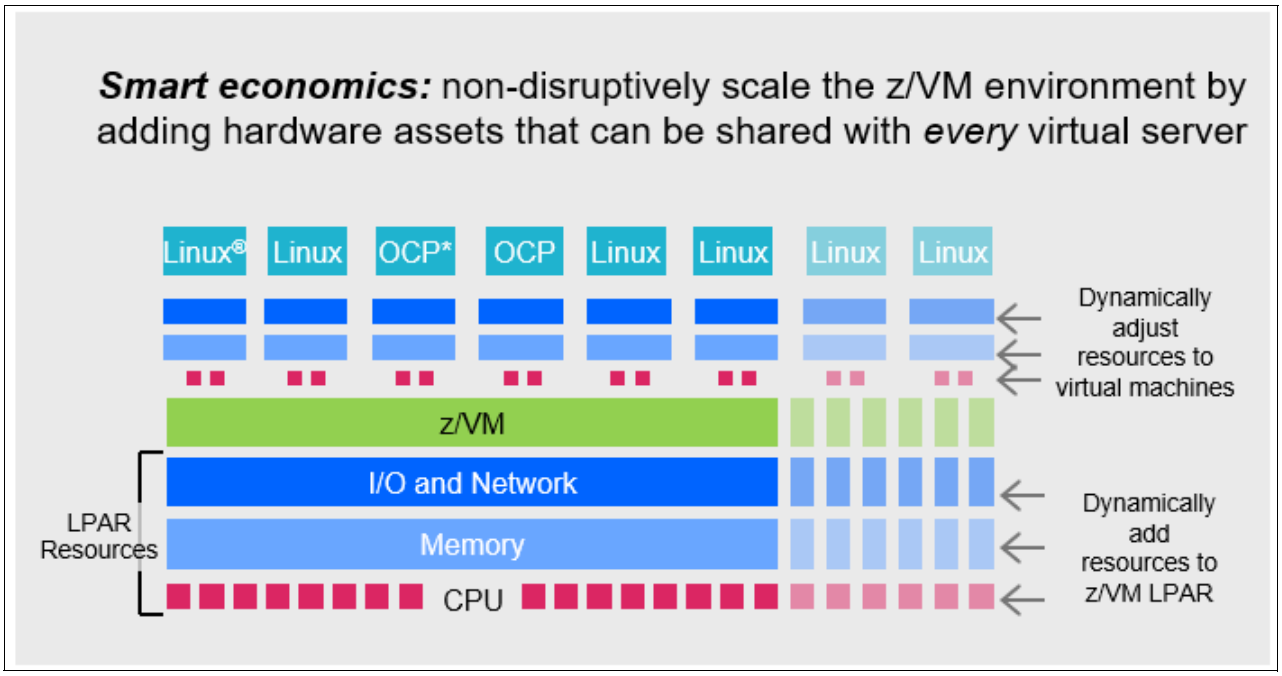


Figure 2-7 Smart economics of the use of z/VM

Other security capabilities on z/VM

z/VM supports encrypted paging in support of the philosophy of encrypting all data that is in-flight and at-rest (available with z/VM V7.1 and z/VM V6.4). Ciphering occurs as data moves between active memory and a paging volume.

IBM RACF® for z/VM provides security systems that include access control and auditing functionality as the backbone for Linux security.

2.3 IBM Secure Execution for Linux

IBM Secure Execution for Linux is a hardware-based security technology that is built into LinuxONE III generation systems. It is designed to protect workloads from internal and external threats to help our clients prevent security breaches. IBM Secure Execution can help protect and isolate workloads on-premises, or on IBM LinuxONE hybrid cloud environments.

Current approaches to security address data-at-rest and data-in-transit. Not many users secure data when it is in use, which creates a window of vulnerability that insiders or criminals can use. Confidential computing is the industry movement around the use of technology to address this vulnerability.

Secure Execution is designed to further this agenda by protecting data that is in-use through the implementation of a hardware-based Trusted Execution Environment (TEE). Hardware-enabled protections can move clients closer to realizing a Zero Trust environment through workload isolation and hardened access restrictions over their data (see Figure 2-8).

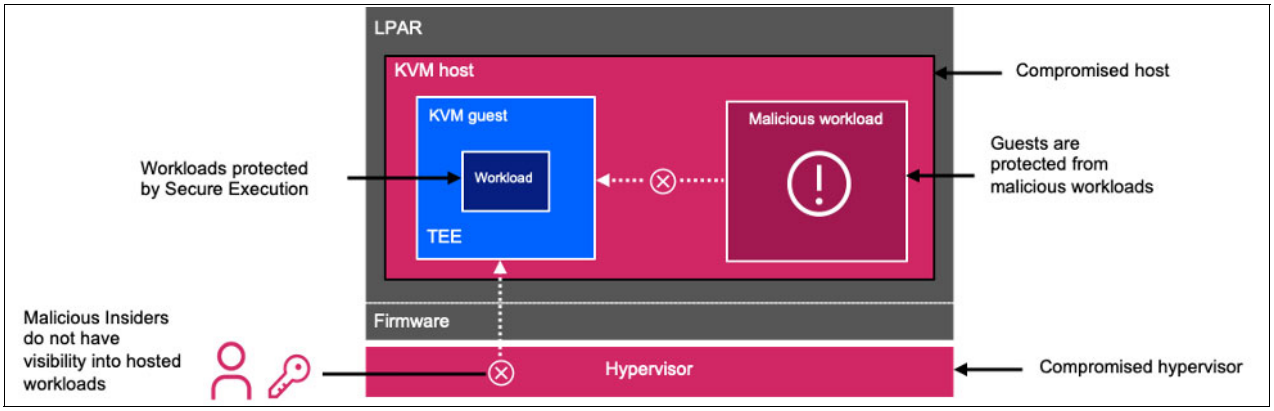


Figure 2-8 Solution overview

IBM Secure Execution for Linux protects your applications and their data from insider threats and external attacks by using the hardware-based environment that is provided rather than using current software-based approaches. By isolating the hardware that is hosting the workloads from the rest of the device, Secure Execution can enable sensitive workloads to run securely on untrusted or compromised infrastructure.

By providing a high level of isolation for workloads, Secure Execution is designed to help prevent security breaches that can result in large financial penalties, regulatory scrutiny, and company discharges.

At its core, Secure Execution provides a KVM-based VM that is fully isolated and protected from the hypervisor with encryption keys to which only LinuxONE hardware and firmware can access. This TEE is designed to protect and isolate workloads better than a standard software environment from internal and external threats.

As more companies move their on-premises workloads to public cloud, the need for a highly secure and trustworthy multi-tenant hosting solution becomes necessary to help support the confidentiality and integrity of each application and its data.

Secure Execution gives you the ability to use hardware-based security technology (TEE) to provide a mechanism by which a hosted workload can run without its memory or execution state being visible to the host or any other workload that is hosted in the same environment.

Enterprises can now protect data and code in-use in their hosted workloads by using protection mechanisms that are offered by Secure Execution. It also provides effective access controls so that only authorized users can access sensitive workloads.

Secure Execution is designed to eliminate the window of opportunity for hosts and guests that are infected with malicious code to use security lapses and gain full privileges to your hosted core business systems. Workload owners can use Secure Execution to help protect sensitive data from corruption and help support data confidentiality and integrity.

For more information about Secure Execution for Linux, see IBM Knowledge Center.

2.4 IBM Secure Boot for Linux

IBM Secure Boot for Linux brings boot integrity to the LinuxONE platform, which is a complete chain of trust from trusted source to boot loader. Secure Boot is part of the Unified Extensible Firmware Interface (UEFI), which is a central interface between the firmware, operating system, and individual components of a computer.

This capability protects your system from root level attacks and viruses that target vulnerabilities during the boot process. The system checks images at boot time for a vendor-signed cryptographic key to verify that the image is from an official provider, and that the image was not tampered with or replaced by malicious third parties.

This feature can be enabled through a simple interface option on the Hardware Management Console. The system firmware first confirms that the system boot loader is signed with a verified cryptographic key. The system then confirms that the key was authorized by a database that is contained in the firmware and only recognized keys allow the system to boot.

3

Users of security on LinuxONE

Building on the secure foundation of the LinuxONE platform, IBM is continuously developing new technology further up the stack that can use the system's industry-leading security capabilities.

Organizations can take advantage of these unique offerings to differentiate their services from competitors with the power and speed that users demand, the security-rich environment that businesses and regulators require, and efficiencies that lower operational expenditures.

This chapter includes the following topics:

3.1 IBM Secure Service Container

The IBM Secure Service Container (SSC) is a solution that hosts container-based applications for hybrid and private cloud workloads and is exclusive to IBM LinuxONE. This secure computing environment can be deployed without any application code changes for the following advanced security capabilities and benefits:

- Tamper protection during installation and start time to protect against malware attacks
- Restricted administrator access to help prevent the misuse of privileged user credentials for cloud and on-premises environments
- Automatic pervasive encryption of data that is in flight and at rest

IBM Secure Service Container uses LinuxONE's EAL5+ certification for vertical isolation of workloads and achieves horizontal isolation that separates the running application from the underlying host environment. Secure Service Container is designed to offer the highest security level available for protected key management (FIPS 140-2 level 4).

IBM Secure Service Container technology builds on the workload isolation of the firmware that is based on LPARs and is unique to IBM LinuxONE. It was used in the IBM Cloud on LinuxONE to provide the advanced security of IBM Blockchain Platform and is now extended for generic container-based applications through IBM LinuxONE.

This technology can be used in an on-premises data center environment through the IBM Hyper Protect Virtual Servers offering. For more information, see this web page.

3.2 IBM Data Privacy Passports

IBM Data Privacy Passports is a consolidated data security solution that protects data after it leaves the system of record, minimizing the risk of security breach, potential noncompliance and financial liability. It provides data-centric protection, which increases organizational control of data by allowing data protection to remain with the data as it is moved from its data source and proliferated across an enterprise.

With this technology, you can implement policy-based, fine-grained data privacy and protection that is attached to data throughout its lifecycle without requiring application changes.

Data Privacy Passports can help your organization:

- Meet regulatory and compliance mandates
- Minimize the enterprise risk and impact of collecting and storing sensitive data
- Control data sharing on a need-to-know basis by using centrally controlled policy

For more information about IBM Data Privacy Passports, see this web page.

3.2.1 Benefits of data-centric protection

Digital business risk is growing because of the challenge of maintaining control over data that is constantly increasing in volume, variety, and value. Meanwhile, cyber attackers are finding increasingly innovative ways to compromise IT infrastructure and steal this data. Because of these risks, it is critical to take measures to protect sensitive data always, even outside the limits of your own data center environment.

The current standard of point-to-point encryption leaves many vulnerabilities and control risks for your data. Encryption and decryption occurs at each location as data traverses the enterprise network. This issue leads to lapses in data protection across hybrid environments and a lack of policy control for your data after it passes over to other systems.

With end-to-end data-centric protection, data is encrypted at its starting point and remains encrypted until it reaches the endpoint. Data that is stored at endpoints and intermediate points are implicitly encrypted and managed through centralized policy.

As a result, only the authorized application or user can view an entitled subset of the data. This solution allows the LinuxONE platform to enable data protection that can span hybrid and multi-cloud computing environments, including data that is stored in public cloud deployments or shared with third parties.

3.2.2 Data Privacy Passports overview

Data Privacy Passports is a data-centric audit and protection (DCAP) technology that can protect data wherever it goes. Security policies are kept and honored whenever the data is accessed. Future data access might be revoked remotely by using Data Privacy Passports long after data leaves the system of record. Sensitive data might even be made unusable by destroying its encryption key.

Data Privacy Passports supports field-level data protection. This support allows for greater granularity and the ability to apply different policy methods for protecting data.

Protected data

Protected data is encrypted to prevent unauthorized access by users who are not approved to view a specific data element. A Passport Controller encrypts raw data into protected data by way of Trusted Data Objects before leaving the platform. This protected data can be down in different views based on the policy rules and the user's need to know.

Enforced Data

After a Trusted Data Object reaches an authorized user, data elements are transformed from protected data into enforced data. Enforced data is masked or redacted to reveal only data that is authorized for a specific user that is based on policy controls that are determined by the central Trust Authority.

Components of Data Privacy Passports

In this section, we provide an overview of the components inside of Data Privacy Passports technology.

Trusted Data Object

A Trusted Data Object contains data that is bundled and portable between multiple environments. Data consumers can freely use data from various sources while access and control is enforced through centrally controlled policy in real time.

Passport Controller

The Passport Controller is a data broker that provides an intercept point to work in cooperation with the Trust Authority to transform raw data into Trusted Data Objects. It also serves to enforce data protection policies. The Passport Controller can be deployed at the data source or the point of consumption.

Trust Authority

The Trust Authority is the central point of control for managing and enforcing data security and privacy. This agent can be deployed independent from the Passport Controller and serves as the center of trust for the Data Privacy Passports solution. An enterprise Trust Authority requires performant, scalable, and robust cryptographic and key management services, which makes it an ideal match for IBM LinuxONE.

IBM is constantly pushing to deliver new ways of addressing upcoming challenges for enterprise data management. The new IBM Data Privacy Passports offering, along with IBM LinuxONE, is designed to enforce security and privacy protections of data across and organization's multi-platform environment. Data Privacy Passports is a consolidated data security technology that protects data after it leaves the system of record, which minimizes the risk of security breach, potential noncompliance, and financial liability.

For more information, see *Protecting Data Privacy Beyond the Trusted System of Record*, REDP-5567.

3.3 IBM Cloud Hyper Protect Services

Built on IBM LinuxONE technology, IBM Cloud Hyper Protect Services provide built-in data-at-rest and data-in-flight protection to help developers easily build applications with highly sensitive data.

These cloud services are infused with enterprise-grade data protection and are made possible by bringing IBM LinuxONE into IBM's global public cloud data centers.

Now, developers and clients can build, deploy, and host applications with an industry-leading data protection that encrypts information that is at rest and in flight. This technology is designed to help protect against threats inside and outside of an organization.

The IBM Cloud Hyper Protect family provides the following services and intends to expand to include others that are crucial for providing protected cloud capabilities:

- IBM Cloud Hyper Protect Crypto-Services
- IBM Cloud Hyper Protect DBaaS
- IBM Hyper Protect Virtual Servers

3.3.1 IBM Cloud Hyper Protect Crypto Services

IBM Cloud Hyper Protect Crypto Services is a key management and cloud hardware security module (HSM). It is designed to enable you to take control of your cloud data encryption keys and cloud hardware security models. It is the only service in the industry that is built on FIPS 140-2 Level 4-certified hardware.

Built on IBM LinuxONE technology, the service helps ensure that only you can access your keys. A single-tenant key-management service with key vaulting that is provided by dedicated customer-controlled HSMs helps you to create encryption keys with ease.

Alternatively, you can bring your own encryption keys to manage. The managed cloud HSM supports industry standards, such as PKCS #11, so that your applications can integrate cryptographic operations like digital signing and validation. Keep your own keys for cloud data encryption that is protected in a dedicated cloud HSM. Maintain control of the key hierarchy, including the HSM master key.

For more information, see this web page.

3.3.2 IBM Cloud Hyper Protect DBaaS

As business leaders look to use the cloud, enterprises in highly regulated industries are concerned about protecting confidential and sensitive customer data. This leading-edge solution offers a highly secure database environment for enterprise workloads with sensitive data. With IBM Cloud Hyper Protect DBaaS, you can provision, manage, maintain, and monitor multiple database types, such as MongoDB and PostgreSQL, through standardized APIs.

Hyper Protect DBaaS is built on LinuxONE technology, which provides built-in data encryption along with excellent vertical scalability and performance. It helps to protect against threats of data breaches and data manipulation by privileged users and provides a high level of data confidentiality for data owners.

For more information, see this web page.

3.3.3 IBM Hyper Protect Virtual Servers

IBM Hyper Protect Virtual Servers is a software solution that is designed to protect your mission-critical workloads with sensitive data from internal and external threats. This offering provides developers with security throughout the entire development lifecycle.

Use this secure cloud service for on-premises and off-premise deployment of mission critical workloads. By using this service, you build once and have the flexibility to deploy anywhere, which gives the same trusted security, availability, and reliability that is expected from IBM LinuxONE. Based on individual needs per workload (resources, time, cost, and so on), you can choose to develop cloud native in a private cloud, public cloud, or a combination of both.

IBM Hyper Protect Virtual Servers includes the following features:

- All images are signed and securely built with a trusted Continuous Integration/Continuous Delivery (CI/CD) flow.
- Infrastructure providers cannot access your sensitive data, but can still manage images through APIs.
- The source that is used to build images can be validated at any time; that is, no back door can be introduced during the build process.

For more information, see this web page.

3.4 IBM Fibre Channel Endpoint security

Fibre Channel is the premier transport for storage area networks. Yet, as with any other component of a datacenter, the need to implement security measures in the SAN exists to reduce and eliminate insider threats of unauthorized access of data. Managing a SAN involves not only providing highly available data access and optimal performance, but it is also essential that all data on the SAN be secure always.

IBM Fibre Channel Endpoint security is an end-to end solution that ensures that all data that is flowing on FICON and Fibre Channel Protocol (FCP) links from IBM LinuxONE to IBM DS8900F or supported SAN Switches and Directors, or between IBM LinuxONE platforms over FICON Channel-to-Channel connections, is encrypted and protected.

This offering provides in-flight protection for all data, independent of the operating system, file system, or access method in use.

End-to-end protection features the following benefits:

- Enabled automatically between host and storage endpoints that are security-capable
- Each established link must “prove” its identity as a trusted component
- Trusted connections are identified; visible to both the Operating System and HMC
- Policy can be established to enforce that only trusted connections can be made
- Each time a link goes down or up, reauthentication or negotiation of device encryption keys occurs
- Integrated key management by using IBM Security™ Key Lifecycle Manager (ISKLM)
- Can be used immediately after Power-on-Reset or enabled later by running IBM LinuxONE with minimal or no disruption.

Because of these benefits, IBM Fibre Channel Endpoint security can help you realize the following:

- Meet regulatory and compliance mandates.
- Minimize the enterprise risk and effect of receiving and storing sensitive data.

IBM Fibre Channel Endpoint security is another data security technology that contributes to the IBM LinuxONE approach of encryption everywhere. It extends the value of pervasive encryption, which further minimizes the risk of security breach, potential noncompliance, and financial liability.

For more information, see *IBM Fibre Channel Endpoint Security for IBM DS8900F and IBM Z*, SG24-8455.

3.5 Cryptographic Key Management for LinuxONE

As described in Chapter 2, “Core security technologies on LinuxONE” on page 15, different types of keys are used for different encryption algorithms. The “Secrecy of Data” is maintained by the encryption keys, not by the encryption algorithms. Although in the early days of cryptography, the encryption algorithm was regarded as the protector of the information, this belief proved to not always be true.

The method of storing keys is important. It is also important how often you change the keys before they get too old. It is often referred to as the '”lifecycle” of a key or a pair of keys that are generated (born), used (lives), and then destroyed or changed (dies).

When keys are created and stored, it also is important to decide who can create and distribute the key and decide on owners for a key that is split into different segments. The National Institute of Standards and Technology (NIST) defines this role as a *key custodian*, and every enterprise must assign that role to a party that is responsible for key lifecycle management.

In this section, we discuss this key lifecycle management in two parts:

- “Operational Key Lifecycle Management” on page 37 - Operational Encryption Key Management with IBM Security Key Lifecycle Manager (ISKLM)
- “Master Key Lifecycle Management” on page 38 - Master Key Management for Crypto Express Adapter with Trusted Key Entry (TKE)

3.5.1 Operational Key Lifecycle Management

Key lifecycle management is a critical aspect in any encryption strategy. Cryptographic keys feature a lifecycle that includes tasks, such as key creation, key activation, key deactivation, key archival, and key deletion. Some regulations, such as European Union (EU) General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI-DSS), and Health Insurance Portability and Accountability Act (HIPAA), require key management processes to be created and well-documented.

Encryption Algorithms and Sharing Keys

When an application must encrypt and decrypt data, it chooses standard encryption algorithms to communicate with other applications and the other entity of the application. Examples of these encryption standards are RSA, DES, AES, ECC, and SHA. Each standard has a specific purpose for its use. When an application encrypts data, it typically uses multiple sets of encryption algorithms to make it more difficult for unauthorized parties to decrypt the data.

For example, if a database uses Advanced Encryption Standard (AES) from the US National Institute of Standards and Technology (NIST) to encrypt its table data, the database also uses the RSA cryptosystem to encrypt the AES encryption key. As a result, the key can be shared with other applications in a secure way.

Many variations and combinations of encryption algorithms exist that can be used and shared. Managing the keys for those methods also varies, but some popular standards, such as the Key Management Interoperability Protocol (KMIP)[1] and Public-Key Cryptographic Standards (PKCS)[2], are available.

IBM Security Key Lifecycle Manager - ISKLM

IBM Security Key Lifecycle Manager (ISKLM) offers a simple integration to your enterprise applications and infrastructures to manage operational cryptographic keys. ISKLM centralizes, simplifies, and automates the encryption key management process to help minimize risk and reduce operational costs of encryption key management. It offers secure, robust key storage, key serving, and key lifecycle management for IBM and non-IBM storage solutions that use the OASIS Key Management Interoperability Protocol (KMIP).

IBM Security Key Lifecycle Manager helps customers meet regulations, such as the Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley, and the Health Insurance Portability and Accountability Act (HIPAA), by providing centralized management of encryption keys.[3]

ISKLM runs on LinuxONE and supports Red Hat Enterprise Linux and SuSE Linux Enterprise Server. It is also integrated with KMIP and PKCS#11. Therefore, you can use it to manage keys for storage devices, such as IBM DS8000®, Spectrum Scale, Virtual Tape libraries, and middleware, such as IBM Db2® for LinuxONE.

For example, if Db2 for LinuxONE is set up to use Db2 Native Encryption, it uses the IBM GSkit interface to use CPACF hardware in CPU to accelerate AES encryptions and decryptions. Db2 Native Encryption also supports KMIP, where ISKLM can be used to manage operational keys for the encryption key lifecycle management.

---

[1] KMIP is an open standard method to standardize the key management within the companies.

[2] PKCS is a set of specifications that were developed for public key cryptography and initially developed by RSA Data Security Inc.

[3] https://www.ibm.com/us-en/marketplace/ibm-security-key-lifecycle-manager

If ISKLM is hosted on a LinuxONE server with the proper JAVA SDK level (that is, JAVA SDK v7/v8), it uses IBMPKCS11Impl to use the Crypto Express Adapter to use hardware acceleration for PKCS#11 functions. You can also use the **`pkcsconf -m`** command to display the supported mechanisms for each slot on a LinuxONE system.[4]

An overview of ISKLM is shown in Figure 3-1.

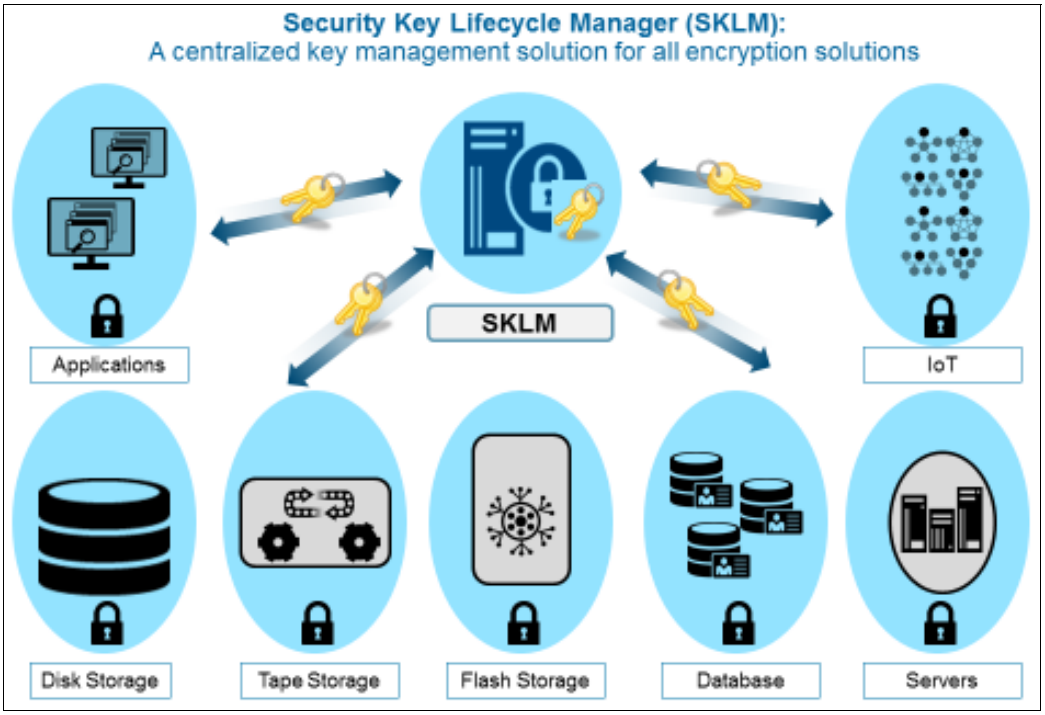


Figure 3-1 ISKLM overview

3.5.2 Master Key Lifecycle Management

The Trusted Key Entry (TKE) workstation is an optional feature of LinuxONE that manages cryptographic keys in a secure environment. The TKE workstation is an integrated solution that contains a combination of hardware, firmware, and software to provide a basic key management tool for the cryptographic coprocessors. TKE securely manages multiple cryptographic modules that run in Common Cryptographic Architecture (CCA) or IBM Enterprise PKCS#11 (EP11) and uses compliant-level hardware-based key management techniques from a single point of control.

Trusted Key Entry (TKE) workstation is a platform that provides convenient way to manage Master Keys in the HSM (in this case, Crypto Express Adapter for LinuxONE).

Master keys on LinuxONE

When a Crypto Express Adapter is configured to wrap an encryption key (that is, a key encrypting key, also known as *secure key*), the root key that is used to encrypt secure keys (also known as the *master key*) is stored in the hardware. This master key that is stored in the hardware never leaves its entity, and is processed only within the hardware to decrypt a key when called by a hardware function. Therefore, a secure key (encrypted key) that is transported into a Crypto Express adapter is used inside that adapter to encrypt or decrypt data with a specific encryption algorithm that is tied to that key.

[4] https://www.ibm.com/support/knowledgecenter/SSYKE2_8.0.0/com.ibm.java.security.component.80.doc/security-component/pkcs11implDocs/ibmpkcs11.html

Many organizations have security policies or specific requirements about how to set the master keys, and how often they should be changed/rotated. Most of the time, the master keys are divided into multiple pieces and distributed to multiple key custodians. At the time of rotating the master keys or generating new master keys, all the key custodians get together along with witnesses to set the new master keys. This process often is called *Key Ceremony*, in which all the required persons get together to securely change the master key. This process adds another layer of security into the process, which makes it more difficult for the keys to be exposed.

TKE: Why do you need it?

You can use a `panel.exe` software tool to change master keys in a Crypto Express Adapter for LinuxONE. It is a free command-line tool that provides a basic interactive session to set up the master keys and change them when needed. For more information about the use of this command-line interface, see the following resources:

- *Getting Started with Linux on Z Encryption for Data At-Rest*, SG24-8436
- The panel.exe utility topic in IBM Knowledge Center

To make a new master key or change the current master key in the HSM, you must enter the current master key into the terminal by using `panel.exe` to load the keys into the Crypto Express Adapter. This method has many potential security exposures because it is connected through the user's terminal to LinuxONE. The keys that are entered on terminal might be exposed in the following ways:

- In host memory on the system where they are entered
- On the network channel for communication to the LinuxONE host
- In host memory for the Linux partition

It also gets tricky to enter all the keys in hexadecimal number form in the terminal without having any errors because one mistake can lead to the loss of an encryption key, which can in turn lead to losing access to the data.

Therefore, IBM is offering the TKS workstation as a solution. It makes the master key management tasks easy and secure compared to the software-only method.

TKE: How it works

Trusted Key Entry is a specialized appliance that is built with custom hardware and software. The hardware is composed of a x86 core-based workstation, which is equipped with a PCI-express cryptographic co-processor. This adapter is the same Crypto Express Adapter that is used in LinuxONE. It also features a pair of smart card readers that are attached so that Master Keys are stored in the smart cards.

The TKE smart panel is shown in Figure 3-2 on page 40.

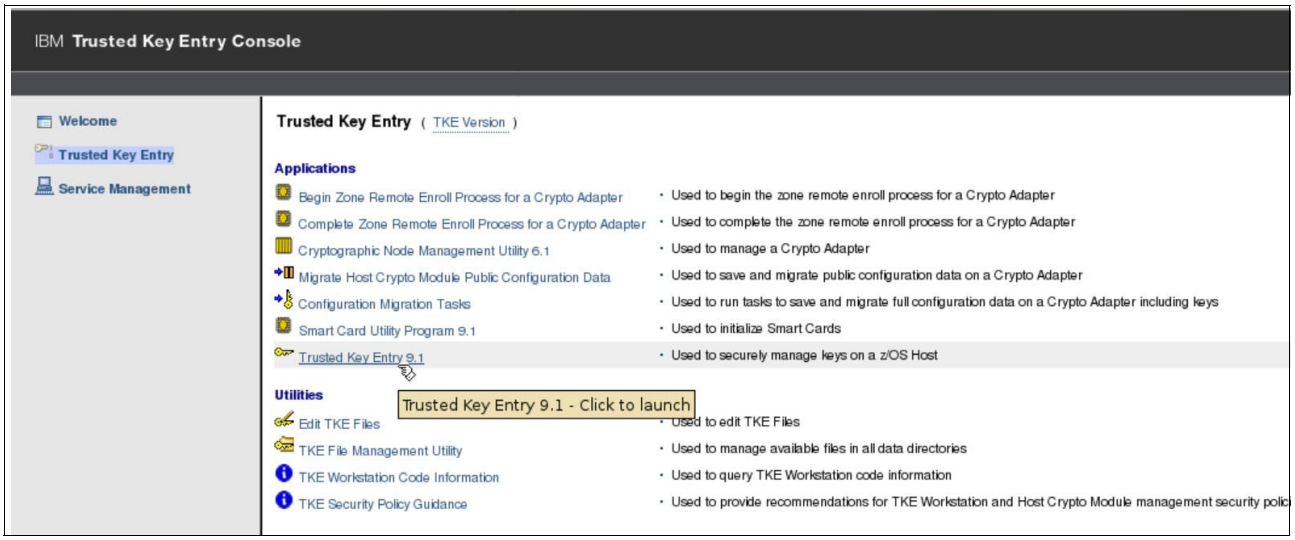


Figure 3-2 Trusted Key Entry Menu panel

The TKE application is designed to give operators and key custodians the most secure way to manage master keys. By using six smart cards (two for certificate authority [CA] cards, two for module [domain] admin cards and two for split master keys), TKE gives maximum security for creating or changing master keys and maintaining them in the most secure format.

A Linux server that runs on LinuxONE has a TKE daemon running that is called `catcher.exe`. This daemon allows the TKE workstation to be connected and communicate downward to the Crypto Express Adapters. By using the GUI on the TKE workstation, each key custodian performs the tasks that each person is assigned to. Figure 3-3 shows the TKE panel with the statuses of various master keys.

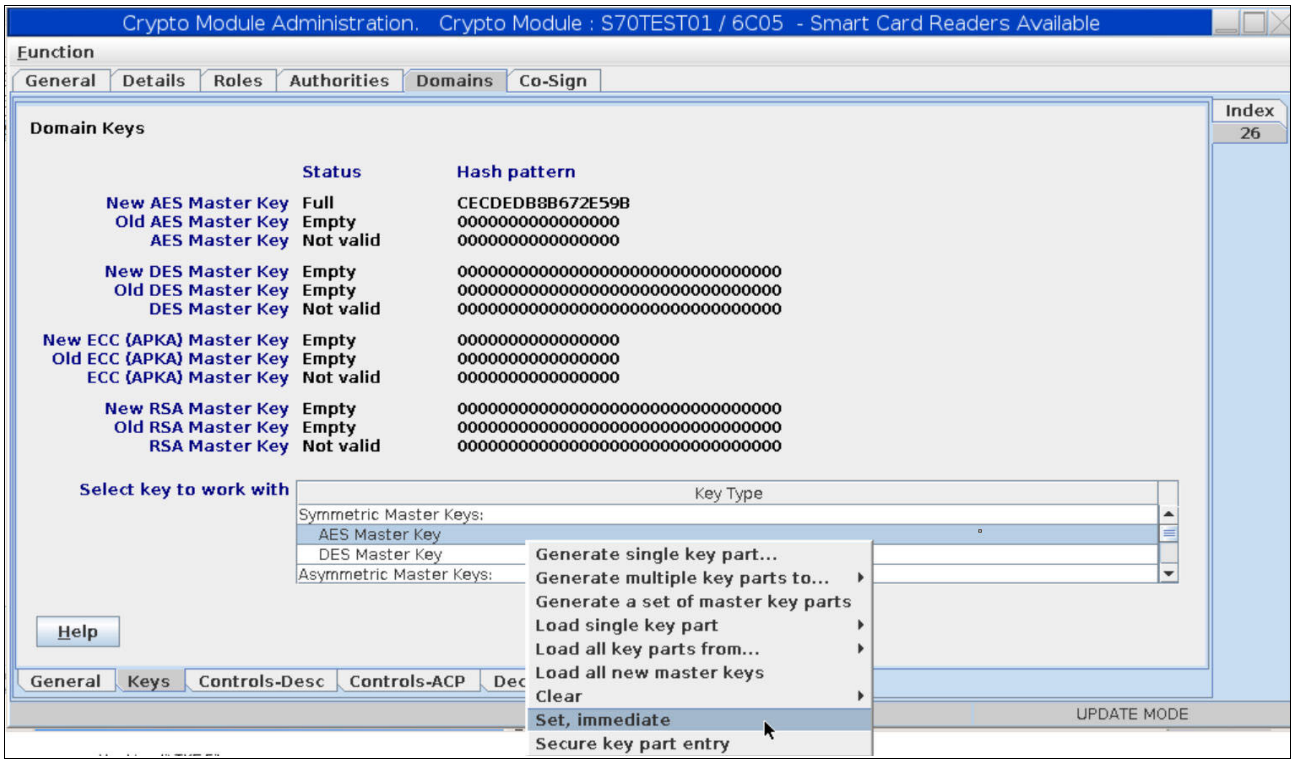


Figure 3-3 Setting the AES Master Key on TKE

Because TKE does not allow a single user to change the master key or allow actions without proper procedures by key owners, this appliance requires the steps that are necessary to provide the most secure way to manage the keys.

The enterprise always must prepare service availability. With data encryption, the production servers and disaster recovery servers must maintain the same master keys, even though they might not be in the same data center. Therefore, after the master keys are created or regenerated in the production servers, they must be loaded into other servers that share and use the encrypted data, including cold-state disaster-recovery servers.

For more information about how to configure and operate TKE, see IBM Knowledge Center.

4

Use cases

In this chapter, we explore examples of encryption use cases that use the security features of LinuxONE. The chapter includes more technical details to help you understand of what occurs “under the hood” of the LinuxONE system.

This chapter includes the following topics:

4.1 Containers and data encryption use case

This chapter describes how you might start to use LinuxONE hardware cryptographic features within a Docker environment and running on LinuxONE. The following sections describe how to benefit from CPACF hardware acceleration to secure client/server communications through an OpenSSL example:

- “Context and challenges”
- “Solution”
- “Implementation” on page 45
- “Summary” on page 49

4.1.1 Context and challenges

We are in an era where container technologies are gaining more popularity. The companies are increasingly adopting this virtualization technology to build and scale cloud-native applications. Undoubtedly, containers provide the flexibility and rapidity to pursue business agility for speed-to-market. This fact is understood and adopted by companies to improve their efficiency and competitiveness.

Docker is one of the most popular container platforms, as it is adopted by companies across all industries to start the journey of cloud transformation. However, this new world of container infrastructure brings many questions about security. Again, IT decision-makers, IT architects, and developers must address all the security concerns that might arise during each phase of containers lifecycle. That way, they ensure the success of the containerization strategy within the company. Some of these security concerns were addressed by different solutions.

If we look at image authenticity, it is possible to use a cryptographic signature mechanism: the Docker Content Trust and Notary functions. This mechanism ensures that a container image is not processed or modified by an unauthorized third party.

If we look at container isolation level, some Linux features, such as namespaces, control groups, AppArmor, or SELinux, can help to keep the containers isolated from each other.

But what about protecting container data? This security concern is a key requirement for companies to comply with regulatory standards when they use containers. Protecting sensitive data in Docker containers can be addressed with encryption. However, this issue again brings us back to the challenges related to data encryption (performance overhead, application changes, and so on). Thus, how can LinuxONE help clients to overcome these challenges that come with the use of containers?

4.1.2 Solution

The first step toward a secure container system is to have a secure host environment with advanced security capabilities to run the entire set of containerized applications.

To help our clients with their journey toward secure hybrid cloud, LinuxONE extends its security features to containers. Thus, containers can use LinuxONE's cryptographic hardware features. Encrypting data applications on containers is simplified and the encryption overhead is significantly reduced after the containers are configured to use CPACF or cryptographic coprocessor cards.

So that containers can use CPACF for hardware accelerated encryption on every core, you must enable access to CPACF in the Docker host where Docker images are deployed. If the Docker host can access CPACF, the Docker containers that run on this host automatically can access CPACF without extra configuration.

The same approach is used for the cryptographic coprocessor cards (Crypto Express adapters) approach. The Docker host must access the cryptographic cards in addition to loading the `zcrypt` device driver. Then, the container images can use the cryptographic cards through the `/dev/z90crypt` device node.

In this document, we use the encryption of data in-flight with OpenSSL as an example to show how to enable and use CPACF function with containers. Figure 4-1 shows the components that are part of the solution for encrypting data in flight with OpenSSL based on CPACF.

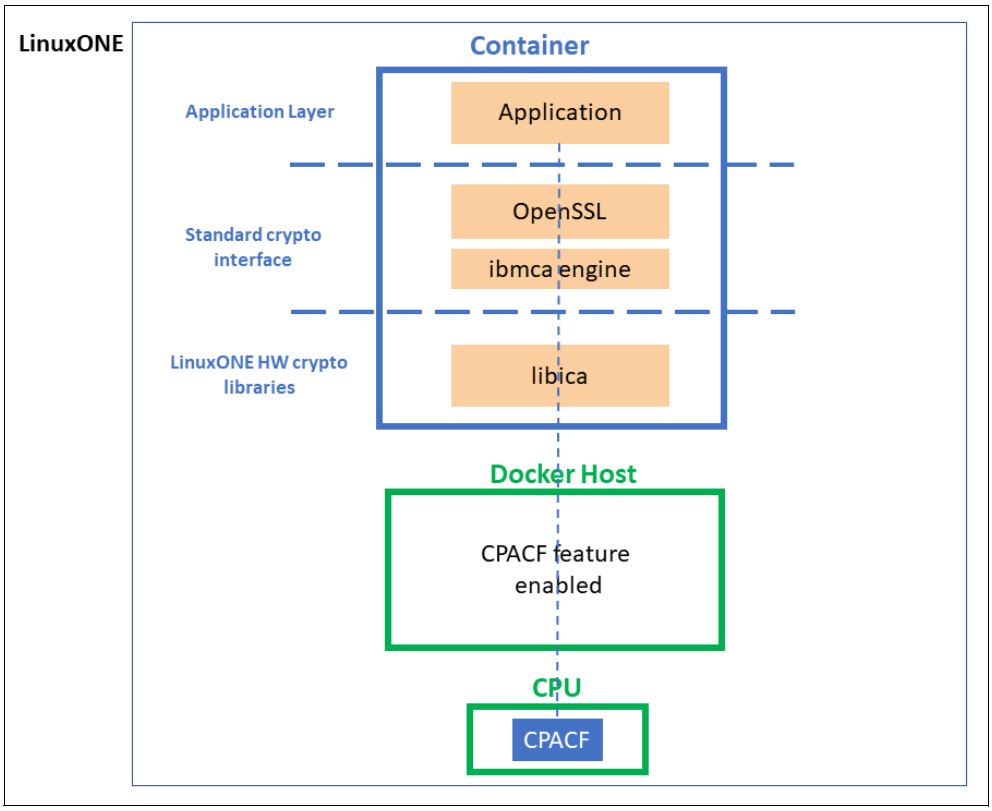


Figure 4-1 Components used for data in flight encryption with OpenSSL

Figure 4-1 also shows an example of containers that are backed by LinuxONE hardware-cryptographic acceleration with CPACF, and the components that are used for data in flight encryption with OpenSSL.

4.1.3 Implementation

In this section, we complete the following steps to enable a Docker container to use CPACF hardware encryption acceleration for OpenSSL.

1. “Checking the CPACF ennoblement in Docker host” on page 46.
2. “Installing required packages in the container” on page 46.
3. “Configuring OpenSSL” on page 47.

For this demonstration, we use a CentOS Linux server release 7.6 for Docker host and container, running on a z/VM LPAR. The Docker image that we use is an image that supports s390x architecture. The ‘s390x’ is used as a suffix by the image providers to specify that the Docker images are compiled for LinuxONE architecture.

Note: For more information about the different options to acquire Docker images for LinuxONE, see IBM Knowledge Center.

Checking the CPACF ennoblement in Docker host

CPACF can be used in your environment if the Licensed Internal Code (LIC) feature 3863 is installed in your LinuxONE. This feature is available at no extra charge. You can confirm that this cryptographic feature is enabled by going directly to the HMC console in one of the following ways:

- Follow the steps that are described in the “Verification of installed LIC 3863 using the SE” section of the IBM Redbooks publication, *Security and Linux on z Systems*, REDP-5464.
- Run the following command in the Docker host:

```
[root@openshiftmaster ~]# cat /proc/cpuinfo | grep features
```

If the `features` list contains **`msa`**, as shown in Example 4-1, the CPACF feature is enabled in the LinuxONE central processors.

Example 4-1 Resultant features list

```
features        : esan3 zarch stfle msa ldisp eimm dfp edat etf3eh highgprs te vx
vxd vxe gs sie
```

Installing required packages in the container

Now that it is confirmed that CPACF is enabled in the Docker host, we know that it is also available automatically to the container. We switch to the Docker container to allow OpenSSL to use CPACF hardware encryption acceleration. For this purpose, we install the following packages, as described next:

- `libica`
- `openssl`
- `openssl-ibmca`

Installing libica library

As shown in Figure 4-1 on page 45, the `libica` library ensures communication between CPACF and OpensSSL. It contains CPACF interfaces that allow applications to use CPACF. Complete the following steps to install the `libica` library:

1. Connect to the Docker container with root user by using the following command, where `2371cdc247ee` is the ID of the container image:

   ```
   [root@openshiftmaster ~]# docker exec -it --user root 2371cdc247ee bash
   bash-4.2#
   ```

2. Install the `libica` library by using the following command:

   ```
   bash-4.2# yum install libica-utils
   ```

The installed `libica` library provides the **`icainfo`** command. You can use this command to display the list of encryption algorithms that are supported by the hardware and therefore available to the container.

Installing OpenSSL library

OpenSSL is an open source cryptographic library that provides an implementation of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. These protocols secure communication between two parties: client and server. Different applications rely on OpenSSL to perform the encryption requests.

To install the OpenSSL library in your environment, use the following command:

```
bash-4.2# yum install openssl
```

Installing the openssl-ibmca library

As shown in Figure 4-1 on page 45, OpenSSL needs the `ibmca` engine to communicate with the `ibmca` library. In this case, the encryption requests are transferred to the `ibmca` engine and not processed directly by OpenSSL. Then, the `ibmca` library communicates with CPACF to allow applications to start using hardware-based cryptographic acceleration.

Install the `openssl-ibmca` library by using the following command:

```
bash-4.2# yum install openssl-ibmca
```

Configuring OpenSSL

Now that all required packages are installed, OpenSSL must be prepared to use the `ibmca` engine. This step is the last step to enable CPACF hardware acceleration of cryptographic functions in OpenSSL.

The `Openssl-ibmca` package contains an `openssl_cnf` configuration file that we use to configure OpenSSL to use the `ibmca` engine. Complete the following steps:

1. Locate the `openssl_cnf` file:

   ```
   bash-4.2# find / -name openssl.cnf /etc/pki/tls/openssl.cnf
   ```

2. Make a copy of the `openssl_cnf` file:

   ```
   bash-4.2# cp -p /etc/pki/tls/openssl.cnf /etc/pki/tls/openssl.cnf.v0
   ```

3. Locate the `openssl.cnf.sample.s390x` file. This file is in the `openssl-ibmca` package. It allows the loading of the `ibmca` engine for all the applications that feature OpenSSL support:

   ```
   bash-4.2# find / -name openssl.cnf.sample.s390x
   ```

4. Add the content of the `openssl.cnf.sample.s390x` file to the `openssl_cnf` file:

   ```
   bash-4.2# tee -a /etc/pki/tls/openssl.cnf <
   /usr/share/doc/openssl-ibmca-1.4.1/openssl.cnf.sample.s390x
   ```

5. Insert a reference to the `ibmca` engine in the `openssl_cnf` file by adding the line `openssl_conf = openssl_def` under `RANDFILE = $ENV::HOME/.rnd` line, as shown in the following command:

   ```
   bash-4.2# vi /etc/pki/tls/openssl.cnf
   # Using the following parameters prevents the configuration file from hanging
   if HOME isn't defined.
   HOME = .
   RANDFILE = $ENV::HOME/.rnd
   openssl_conf = openssl_def
   ```

6. Confirm that the support of `ibmca` engine is enabled for OpenSSL. The `ibmca` engine must be listed in the result of the following command, as shown in the right column:

```
bash-4.2# openssl engine
(dynamic) Dynamic engine loading support
(ibmca) Ibmca hardware engine support
```

Testing the CPACF hardware encryption acceleration in the container

To verify that your container was properly configured to use the CPACF hardware encryption acceleration with OpenSSL, run the following command:

```
bash-4.2# openssl speed sha1 -elapsed | tail -n 3
```

The results of that command are shown in Example 4-2.

Example 4-2 Verify that container is configured to use OpenSSL with sha1 encryption algorithm

```
You have chosen to measure elapsed time instead of user CPU time.
Doing sha1 for 3s on 16 size blocks: 6411336 sha1's in 3.00s
Doing sha1 for 3s on 64 size blocks: 5656337 sha1's in 3.00s
Doing sha1 for 3s on 256 size blocks: 4747020 sha1's in 3.00s
Doing sha1 for 3s on 1024 size blocks: 2938084 sha1's in 3.00s
Doing sha1 for 3s on 8192 size blocks: 612107 sha1's in 3.00s
The 'numbers' are in 1000s of bytes per second processed.
type             16 bytes     64 bytes    256 bytes   1024 bytes   8192 bytes
sha1             34193.79k   120668.52k   405079.04k  1002866.01k  1671460.18k
```

To verify that the OpenSSL cryptographic calls are using CPACF, run the following command:

```
bash-4.2# icastats
```

Typical results of this command are shown in Example 4-3.

Example 4-3 Results of icastats command

```
 function     |           hardware       |            software
--------------+--------------------------+-------------------------
              |      ENC    CRYPT   DEC  |      ENC    CRYPT   DEC
--------------+--------------------------+-------------------------
        SHA-1 |        34525344          |                0
      SHA-224 |               8          |                0
      SHA-256 |               8          |                0
      SHA-384 |               8          |                0
      SHA-512 |               8          |                0
    SHA3-224  |               0          |                0
    SHA3-256  |               0          |                0
    SHA3-384  |               0          |                0
    SHA3-512  |               0          |                0
   SHAKE-128  |               0          |                0
   SHAKE-256  |               0          |                0
```

Notice that the hardware column in Example 4-3 shows that the OpenSSL cryptographic calls are using CPACF.

4.1.4 Summary

In addition to the advantages related to scalability and performance, LinuxONE provides your containerized applications with a secure host environment. By running your containers on LinuxONE, you can benefit from its hardware security features to secure and accelerate the encryption of your data. One of the main advantages of the use of these hardware security features is encrypting your data without modifying your applications and with minimal performance overhead.

The use of OpenSSL for data in-flight encryption is one of the various examples of what you can implement on LinuxONE. You also can use other Linux libraries, such as `dm-crypt`, to encrypt your data at-rest while you continue to benefit from the hardware cryptographic acceleration with CPACF or cryptographic cards.

With its differentiating security capabilities, LinuxONE is a great starting point in your transition to cloud-native applications. LinuxONE also can help you meet compliance requirements for protecting sensitive data in a container system.

4.2 Database and volume encryption use case

This section describes how you can use LinuxONE hardware cryptographic acceleration capabilities features to address the challenges that are related to protection of sensitive data that is stored in databases. This approach is illustrated through a database volume encryption use case with `dm-crypt` LUKS- and CPACF-protected keys to protect data at-rest.

4.2.1 Context and challenges

Databases contain different types of sensitive information, including the following examples:

- Personally Identifiable Information (PII), which is related to data that can help to identify a specific individual.
- Business Information that includes data that represents a risk to the company if disclosed to competitors or the general public.
- Classified Information that refers to top-secret government data.

All these types of sensitive data must be protected, especially in the light of data breaches that are affecting more businesses. Different regulations and laws exist to ensure that this sensitive data remains in good hands. Otherwise, companies can incur heavy financial repercussions.

All these factors make the protection of data that is stored in databases more urgent and important in our century. It becomes one of the highest priorities for companies around the world.

This context brings back a significant focus on data-at-rest encryption. This focus addresses some of the data security issues and complies with various regulations, such as Payment Card Industry Data Security Standard (PCI DSS) or the Health Insurance Portability and Accountability Act (HIPAA).

Consider the following scenario. Your company uses a database that stores sensitive information. To meet the data protection requirements, you must encrypt all data in-flight and at-rest. How you can meet this requirement without altering your applications' response times, increasing your costs, or suffering from lack of skills in your organization?

For data in-flight, these issues can be easily addressed by encrypting your data based on SSL encryption by using the OpenSSL Linux library, for example. On LinuxONE, OpenSSL can benefit from the hardware cryptographic acceleration with CPACF or cryptographic cards. Thus, you can transparently encrypt connection by the database server, in addition to securing the Linux sessions through SSH, for example.

Regarding the protection of data at rest, one of the most common use cases is the use of Filesystem-level encryption, which encrypts data before it is written out to physical volumes. However, this option can expose you to the same issues (costs, performance impact, and so on). Thus, how can LinuxONE help you to minimize the effect of encrypting your data at-rest?

4.2.2 Solution

Encryption at the file system level can be implemented by using `dm-crypt` LUKS, which is an encryption subsystem that is included in the Linux Kernel. With this transparent encryption mechanism, you can encrypt disks, software RAID volumes, partitions, and logical volumes to protect your data at rest. It allows the encryption of all data that is written to disk and decrypts all data that is read from disk. The data appears only in the clear in the application.

Note: The `dm-crypt` provides plain format volumes or Linux Unified Key Setup (LUKS) volumes. In plain mode, `dm-crypt` does not add any headers or metadata to the volumes. The `dm-crypt` LUKS adds a metadata header to the encrypted volume data, and therefore offers more features than plain mode.

LUKS2 format is the preferred option for LinuxONE data at-rest encryption. For more information, see 3.9.3, “Volume format considerations” in *Getting Started with Linux on Z Encryption for Data At-Rest*, SG24-8436.

By implementing this encryption option on other platforms, you might see increased performance overhead, which is always involved when you use software-encryption mode. On LinuxONE, `dm-crypt` LUKS can use the CPACF on-chip encryption co-processor to remove this overhead.

LinuxONE also provides a unique security enhancement for `dm-crypt`, which consists of the use of the CPACF protected keys support to resolve the security issues that are related to storing keys. If `dm-crypt` is used with clear key, keys are readable if the memory system is dumped. With a CPACF protected key, no encryption key is stored in clear in the operating system.

The `dm-crypt` cryptographic operations are performed by using CPACF. CPACF code generates the wrapping keys. These keys are unique to each LPAR, and they are stored in the Hardware System Area (HSA). HSA is a reserved memory area that is separated from client-purchased memory that is used for internal system functions. HSA also is accessible through only the firmware.

As shown in Figure 4-2 on page 51, at the cryptographic card level, the secure key is encrypted by the master key. This secure key is used as the source key of the protected key. It is decrypted and sent to CPACF in clear text. Then, at CPACF level, the key is wrapped by the CPACF wrapping key, and the protected value is stored in memory. As a result, protected keys can never be seen in plain text by the operating system or by applications. With each encryption or decryption operation, the protected keys are sent to CPACF to be unwrapped by the CPACF wrapping keys.

Figure 4-2 shows an overview of data-at-rest encryption that uses `dm-crypt` on LinuxONE. It also shows that `dm-crypt` is located between the file system and the physical disks, which allows data encryption to happen when they are written to physical disks.

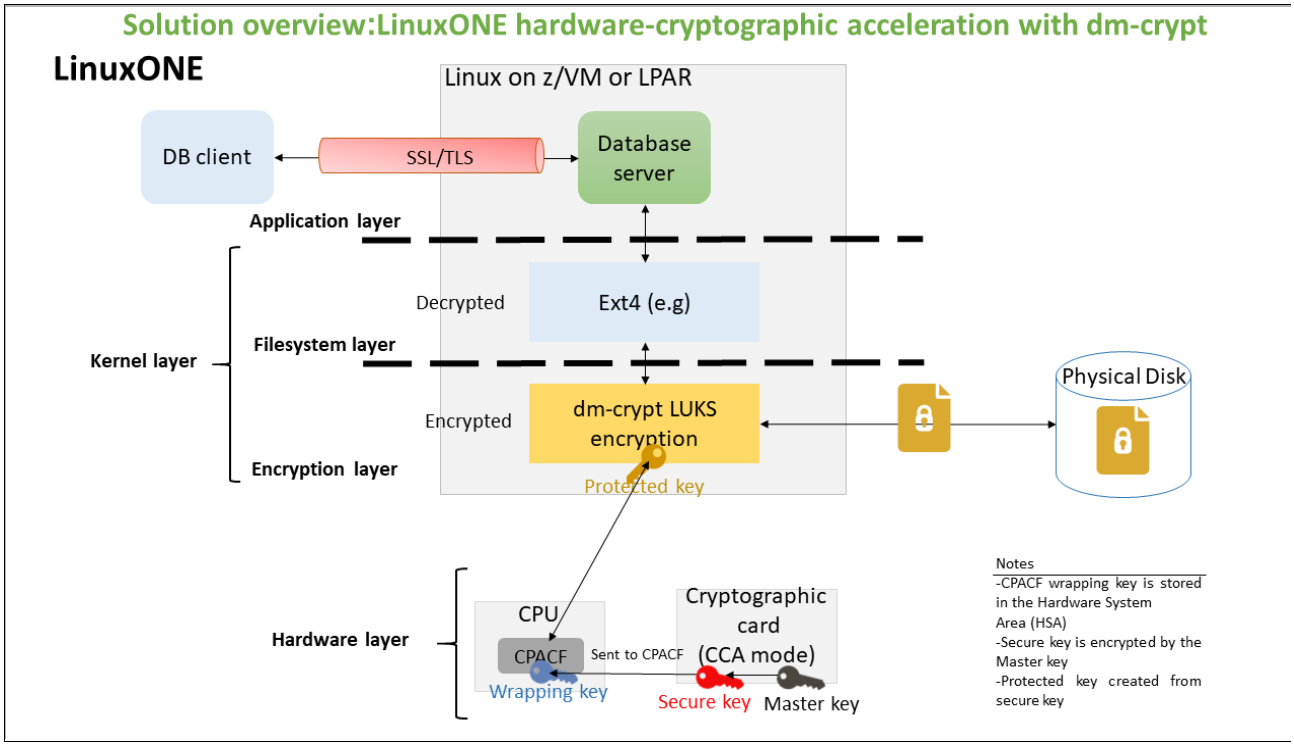


Figure 4-2 Solution overview: LinuxONE hardware-cryptographic acceleration with dm-crypt

Figure 4-2 also shows the key wrapping process that is used to provide `dm-crypt` with CPACF protected keys.

4.2.3 Getting started

The following steps refer to the main steps that compose the data at-rest encryption process that uses `dm-crypt` LUKS with CPACF protected keys.

1. Check CPACF enablement in your system. Licensed Internal Code (LIC) feature 3863 must be installed.
2. Check the availability of Crypto Express adapters (use CCA mode), and add the domains that are needed to hold the master key and secure key. (This process can be done by using the HMC console.)
3. Load the master key into the Crypto Express adapter domain.
4. Install the `pkey` kernel module for protected key management.
5. Use the `zkey` utility to generate and manage secure key.
6. Set up `dm-crypt` as usual (install the `cryptsetup` package).
7. Create the encrypted volumes and set up the `dm-crypt` LUKS2 header in the volumes.

For more information about these steps, see *Getting Started with Linux on Z Encryption for Data At-Rest*, SG24-8436.

4.2.4 Summary

As an enterprise data-serving platform, LinuxONE provides a secure environment to protect the sensitive data that is stored in your databases. Protecting data at rest is one of the important components in the Data Security journey. To help clients with the different challenges that are related to the implementation of data-at-rest encryption, LinuxONE offers hardware cryptographic acceleration capabilities with CPACF.

Encryption of database volumes with `dm-crypt` LUKS is one of the solutions that can be implemented on LinuxONE to protect your data at rest. That type of protection is one of the most common use cases. Because this mechanism works at the kernel level, it can improve security in the following fundamental areas:

- Performance: You avoid the overhead that is associated with traditional encryption.
- Encryption: You better protect the encryption keys against eventual attacks by using the protected keys that CPACF provides.

4.3 Hyper Protect Digital Asset Platform

In the early days of Bitcoin's introduction, crypto currency and blockchain technology were recognized as somewhat interchangeable. As the industry and community adopted crypto-currency and understood its uses better, it is clear that the two technologies serve different purposes.

Blockchain on the enterprise side was adopted as a distributed ledger; for example, Linux Foundation’s Hyperledger project.

As individuals, private sectors and governments acknowledged this type of alternative currency likely is to remain. Also, many architectures and practical implementations were proposed to protect digital assets, such as crypto currencies.

IBM recently announced Hyper Protect Digital Assets Platform, which uses IBM LinuxONE’s strong security features to protect those digital assets against any intrusions.

4.3.1 Digital assets and why is it important

Bitcoin was developed by Satoshi Nakamoto as a form of peer-to-peer electronic cash transactions. He saw the problems of current (at the time) electronic payment systems, and wanted to solve the issue with his invention of a peer-to-peer distributed transaction system, without any central authority involved.

Since Bitcoin’s genesis block was created over 10 years ago, many other crypto currencies were introduced, and disappeared. Many crypto currency-related businesses were founded and one popular area was crypto currency exchanges in which central bank-managed currency can be converts into a crypto currency and vice versa.

Some instances exist of crypto wallets being stolen, or even an owner of the crypto currency exchange passing away while no one else knew the master encryption key for the crypto-currency asset repository.

Now, imagine what similar situations can happen to you even if you do not own any crypto currencies. If you use any coffee franchise application, they might feature their own rechargeable wallets 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 or points and loses them, there is almost nothing your central or local bank can do because it is out of the governed and regulated system. After you purchase points, it is a completed transaction from the store's perspective.

As another example, we review application-based money transfers. More banks allow people to transfer money to other banks by using their own franchised money transfer applications. You need only the recipient's email or phone number but no bank routing and account number to make the wire transfer. Some countries even use their wireless phone company to manage money transfers and make payments, even bypassing banks.

Many online payment companies enable the use of their application to charge central currency into their central system and make payments or transfer to anyone that uses the same application. You can think of all of these applications as *digital assets*, where a valued asset is stored in digital format and can be moved from one owner to another easily and quickly without a traditional central agency being involved.

Digital assets are also not only currency but anything that represents ownership of physical assets someone or organization can own legally, such as property titles or deeds that are transformed into digital form (that might contain digital signatures), or even intellectual properties that do not feature any associated physical properties.

If an incident (including cyber attacks) occurs to a system that stores these digital assets, such as deeds, it can be catastrophic if no other way method exists to restore proof of ownerships or the property.

Many countries, including the US, are making efforts to understand how Central Bank Digital Currency (CBDC) can work for them and how to properly prepare for the next generation of currency exchanges and safeguarded infrastructures. If or when a central bank announces a plan for digital currency, it might greatly affect private banks and accompanied payment systems. Because it has a potential to adopt Satoshi Natakmoto's idea of peer-to-peer payment system, it is critical to understand how a digital asset exchange enterprise can ensure that 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. Next, we describe how the proposed architecture with Hyper Protect Digital Asset Platform works.

4.3.2 Hyper Protect proposed solution architecture

In this section, we examine a proposed solution architecture.

Root of Trust: Keeping the master key secure

As described Chapter 2., "Core security technologies on LinuxONE" and Chapter 3., "Users of security on LinuxONE", IBM LinuxONE offers a strong hardware security module (HSM) by a Crypto Express adapter (CEX).

By using the CEX, Hyper Protect Crypto Services enables you to keep and manage operational encryption keys secure. Those keys are encrypted with your own master key that is visible only to you and never leaves the hardware (HSM, CEX in LinuxONE, and so on).

The master keys can be backed up using smart cards through another secured service that is called Trusted Key Entry (TKS) as described in Chapter 3., "Users of security on LinuxONE". This master key management with encrypted operational keys provides the "root of trust" to make Hyper Protect Digital Asset Platform most secure.

Providing secure application hosting server: Vertical security

Now, the digital asset management application (we call it a *digital wallet application* or *hot wallet* here) runs on LinuxONE's Hyper Protect Virtual Server. This server starts with tamper resistant secure start process, and the storage that is accessed by the virtual server is encrypted with a protected key. This protected key is decrypted only in a special memory area of LinuxONE. When access to the encrypted disk is needed, encryption or decryption of data that is transferring in or out of the disk is run.

After the server is up, it deploys a container image that is also encrypted and signed by the Secure Build process. During the build process of the secure Docker (or equivalent OCI-compliant container) images, many security checks and endorsement are performed to ensure no malicious code is being implanted, and the application code that is saved in the container is a legitimate application from the software vendor (in this case, a digital wallet application).

If any reason exists to capture the memory dump from Hyper Protect Virtual Server for debugging purposes, the memory dump also is encrypted. Therefore, you must use a private key to access the encryption key for the memory dump. This feature is a key differentiator for LinuxONE compared to other platforms.

Communicating between container images by using secure channel: Horizontal security

Because Hyper Protect Virtual Server can limit the login access to an operating system shell, the server communicates externally only with APIs. Secure communications channels also can exist between application containers that use secure protocols, such as mTLS.

The asymmetric key pairs for applications and APIs are managed by EP11 over gRPC (GREP11) where the master key for EP11 service also comes from the HSM (Crypto Express card), which provides maximum protection of asset transfers when a digital asset is transferred by using the user's private/public key pair.

If the digital wallet must be a cold wallet (that is, a wallet that is offline and used for storing crypto-currencies), the master key that is stored in HSM is zeroed out to make all the access to the assets inaccessible. The cold wallet can be accessed again after the master key is restored with key restore ceremony.

Pervasive Encryption Pyramid for LinuxONE

Either from external or internal threats, the security of applications must be protected from all possible accessible threats by bad actors. Hyper Protect Digital Asset Platform architecture provides maximum security protection of every layer that any security professional would want to adopt.

When IBM LinuxONE was designed, it was proposed to achieve maximum security with an 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 a good example of how enterprise applications can achieve Pervasive Encryption with LinuxONE.

Figure 4-3 shows how IBM LinuxONE's Pervasive Encryption Pyramid is matched with Hyper Protect Digital Asset Platform. You can see it provides end-to-end full data protection over various layers of infrastructure and application layers.

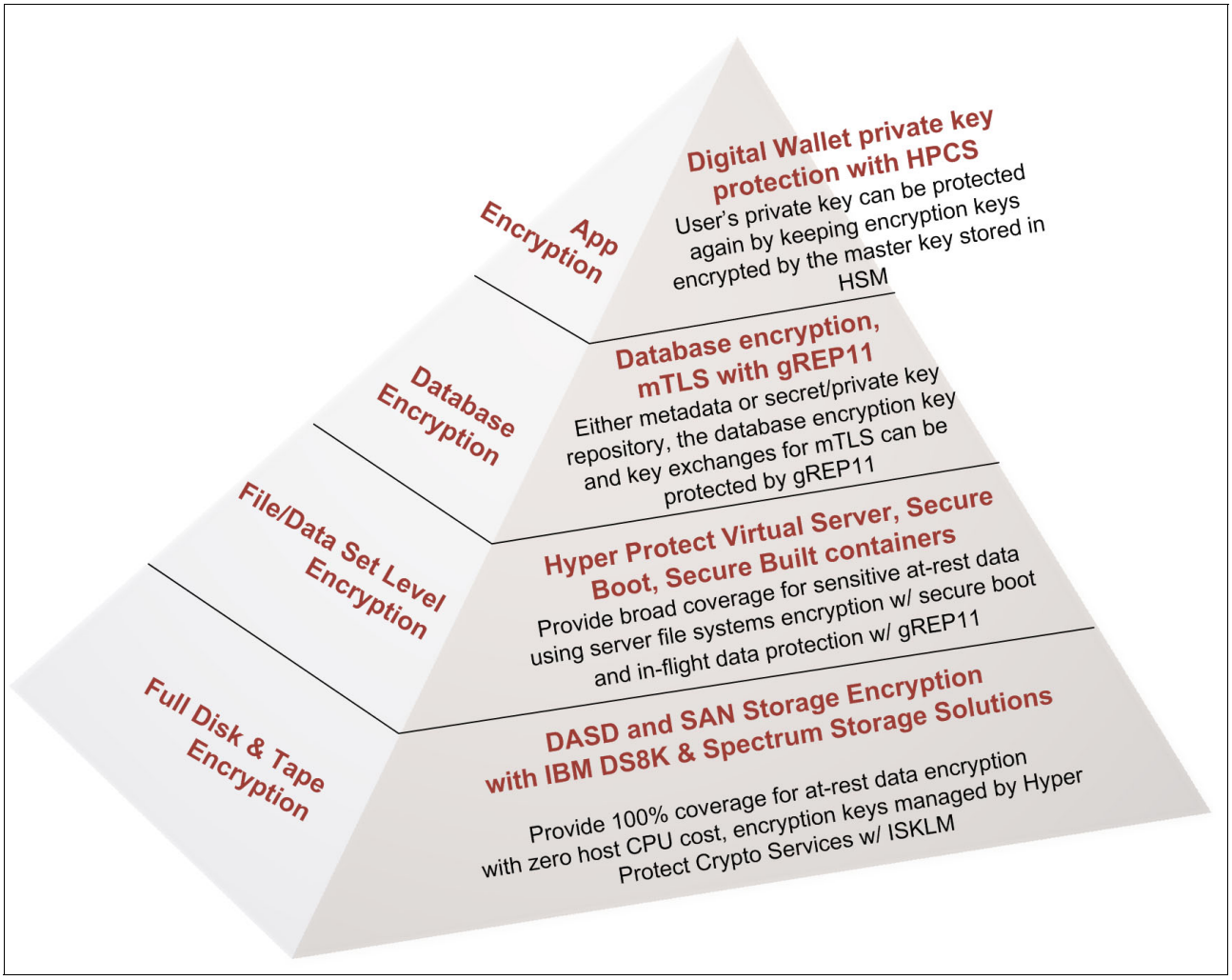


Figure 4-3 LinuxONE Pervasive Encryption with Hyper Protect Digital Asset Platform

4.3.3 Solution offering and deployment examples

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

Figure 4-4 on page 56 shows how IBM Hyper Protect Digital Asset Platform is offered on-premises with IBM LinuxONE or from IBM Cloud.

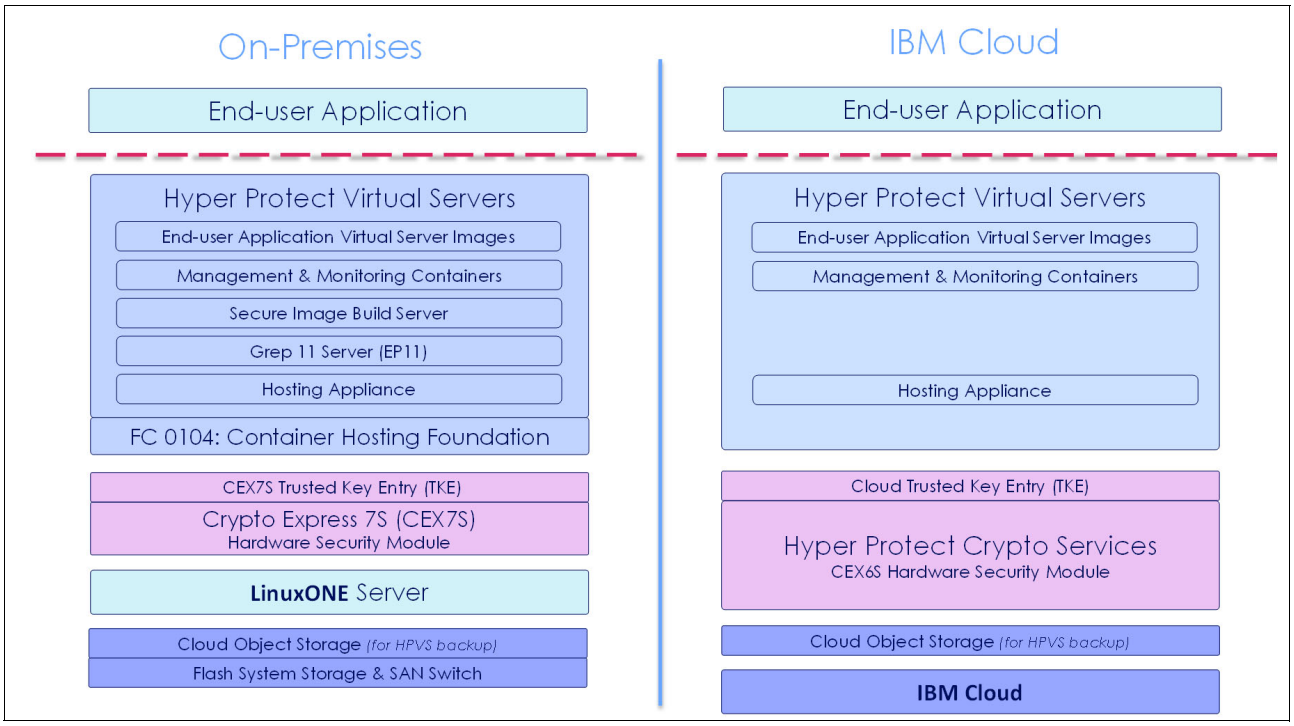


Figure 4-4 IBM Hyper Protect Digital Asset Platform Offerings

Many LinuxONE clients deployed Hyper Protect Digital Asset Platform, including the following examples: For more information about the Hyper Protect Digital Asset Platform, see this web page.

- Hex Trust is a financial technology startup migrating production institutional digital asset custody solution to on-premises custody-as-a-service.
- hOnChain Custodian is another financial technology startup that uses IBM Cloud Hyper Protect Crypto Service to offer cloud-based institutional digital asset custody.
- Kore Technologies is a financial technology startup that is based in Switzerland. It offers an on-premises and cloud-based enterprise grade digital asset custody and issuance solution.
- DACS is also a financial technology startup in South Korea that builds on-premises LinuxONE native institutional digital asset self-custody and trading solutions.

For more information about the Hyper Protect Digital Asset Platform, see this web page.

5

IBM Blockchain Platform with IBM LinuxONE

The IBM Blockchain Platform (IBP) provides an easy way to create and deploy Hyperledger Fabric servers in the public cloud or in an on-premises data center.

In this chapter, we describe how an enterprise client can deploy IBM Blockchain Platform. We also and explain the security benefits of building a blockchain on LinuxONE.

This chapter includes the following topics:

5.1 Blockchain, Hyperledger, and IBM Blockchain Platform

Well-known from its use for crypto currencies, such as Bitcoin, blockchain technology is a hot topic in the technology industry. The core components of blockchain technology are not new. However, as computing power grew alongside the expansion of IoT and mobile devices, adopting blockchain technology into applications became a feasible reality. Blockchain can provide a way for enterprises to share data among one another securely, but also apply permissions on who can create and view that data.

Blockchain technology provides a way to securely store data, most of the time as a metadata to point to more detailed database tables. The data that is stored in blockchain is distributed among participants' servers, which are also called *decentralized data stores*.

Data that is stored in blockchain is also inherently encrypted with strong cryptographic algorithms and key management procedures. When a blockchain stores data with these cryptographic procedures, it stores them with time stamps, which is sequence information that indicates the order of the data blocks, and hash information that is derived from a previous data block. As a result, it can prove its position in the blockchain that is based on its parent block.

This strong cryptographic process makes blockchain "immutable", which means that after data is stored, it stays in its original form and cannot be modified. Unlike other commonly used databases, blockchain normally does not allow inserts or modification of its data. For this reason, blockchain is a strong candidate for verified ledger applications between many distinct parties.

Large enterprises in industries, such as banking, insurance, supply chain and logistics, and healthcare are thinking about how they can adopt blockchain technology. IBM worked with these customers on requirements for blockchain technology. During that process, IBM discovered that public network blockchain protocols, such as Bitcoin and Ethereum, were not a good fit for enterprise use cases.

IBM researchers and developers worked to create a foundation of enterprise-grade private blockchain protocol and donated the initial work as an open source software to the Linux Foundation, which became the Hyplerledger Fabric. Although it is still possible to run other types of open source blockchain protocols in LinuxONE, no formal support is available; therefore, it is not covered here.

IBM created IBM Blockchain Platform, which is an easy way to create and deploy Hyperledger Fabric servers in public cloud or in an on-premises data center.

Hyplerledger blockchain was created from the needs of the enterprise. It is a permission-based private blockchain network. Therefore, only allowed participants can see the data and access the data from the shared, distributed ledger (database).

We describe the basic concept of blockchain data next.

Figure 5-1 shows how each block of data on a blockchain network is stored in each peer node's database. A peer node is served as data processing host for the blockchain network. It validates and endorses a transaction that is requested from an application. Then, it ensures that the rules (business rules) that are described in chain code are checked when the transaction occurs.

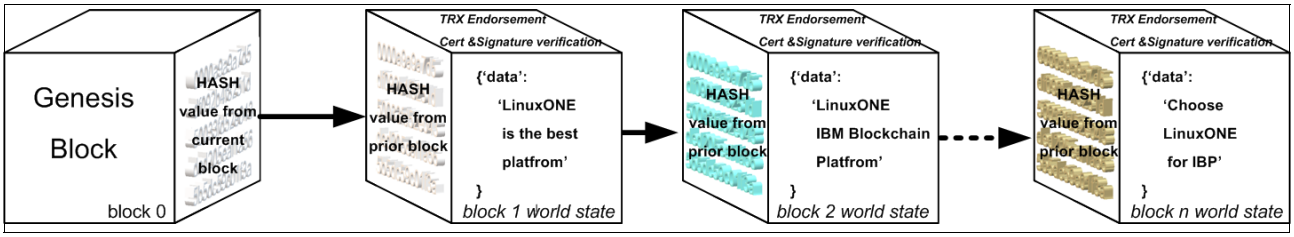


Figure 5-1 High-level concept of Hyperledger blockchain data creation

The peer also communicates with the orderer unit, where it keeps the sequence of transactions and distributes to proper peer nodes when a transaction is requested.

A certificate authority also is available that manages certificates for each member's entity to verify that it is genuine and to validate authenticity.

On a peer node, the blockchain always starts with a genesis block, which is an initial data block that includes a specially encoded hash value. Its hash value is also transferred to the next block in sequence as an input. The next block generates a new hash value from the previous block's hash and the payload of the new block's data; then, it repeats for the next blocks.

Keeping the previous block's hash and making a new hash from it makes blockchain data unable to be reversed or modified. When the contents of the data payload (world state) changes, blockchain changes the hash for the next block that was created and affects all of the world states behind the block that was modified. This idea is the key idea of blockchain data being immutable and it requires a high-speed hash process to generate new blocks.

Hyperledger also uses an asymmetric cryptographic function to create certificates and validate the signature of the transactions. The workflow of those asymmetric keys can be complicated in Hyperledger Fabric because it involves multiple members and different channels for various application uses.

If a person or an organization plans to develop Hyperledger applications, they must plan carefully where to host the service because it can use a large amount of resources, depending on transaction sizes.

IBM LinuxONE is a great choice for a large enterprise Hyperledger Fabric service platform because it features the best cryptographic hardware in the industry. Also, it includes a feature that is called *On/Off Capacity on-demand*. You use it to enable extra CPU capacity to boost processing power in a few seconds for any need that is caused by spiking workloads.

For more information about Hyperledger blockchain network, see this web page.

5.2 IBM Blockchain Platform for LinuxONE

To run a Hyperledger application for your enterprise, or even for personal projects, you need to have at least one Hyperledger Fabric Network running somewhere. It is an architecture form that consists of multiple servers and services. They require many different access controls, permissions, and business rules. In the Hyplerledger world, these business rules are called *Smart Contracts*, and it is represented in the form of *Chain Code* ("chain" as in "blockchain").

You can choose to download the open source version of Hyperledger codes to your personal computer or your choice of servers. If you are an enterprise blockchain application developer or architect, you need at least have one Hyperledger Fabric Network running across your team to develop and test more extensively.

When the business applications interact with other business entities, the Hyperledger Fabric must serve those other entities over the internet and communicate to handle the chaincode's requests. This task often is not a simple. Although you are running multiple servers, they must always be up and redundant to keep the data replicated and consistent among participating members of the blockchain network.

For this reason, IBM Cloud hosts Hyperledger Fabric services to enterprise customers with 24x7x365 support, as a solution called IBM Blockchain Platform (IBP). You can choose to start coding from IBP in IBM Cloud, but you also can download container images for IBP and run them on your on-premises server.

5.2.1 IBM Blockchain Platform

The IBM Blockchain Platform (IBP) is a Hyperledger Fabric blockchain protocol as-a-service that has following properties (for more information, see this web page):

- Modularity

  Blockchain networks must incorporate a wide range of new and existing "pluggable" features, depending on the enterprise and industry. As a result, Hyperledger Fabric was developed to be modular to support networks as new features emerge. Modularity in Hyperledger Fabric allows the IBM Blockchain Platform to use industry-leading security practices to serve production-ready networks, including GDPR and HIPAA best practices.

- Scalability

  Organizations across industry sectors demand solutions that scale as they move past initial explorations and proof-of-concepts.

  Hyperledger Fabric was built to support growing business networks, which must dynamically add participants and support. These additions increase the amounts of transaction processing. Many aspects of scalability depend on the network configuration of consensus, membership, and security. The IBM Blockchain Platform uses Hyperledger Fabric to provide a modular platform that supports the ability to configure a network to support the throughput numbers and network growth that are required.

- Consensus

  An important feature in the security, scalability, and maturity of any blockchain framework is a clearly-defined and implemented consensus protocol. Consensus in Hyperledger Fabric is pluggable and fit specific enterprise use cases.

Therefore, Hyperledger Fabric allows you to choose the best consensus protocol to fit your specific business networks' needs. Hyperledger Fabric's success to date is driven by the massive amount of community support it received through Hyperledger. Open governance of the code base with a clear purpose allowed it to emerge as the industry-leading protocol and framework for enterprise production networks.

Although IBM Blockchain Platform is offered in IBM Cloud and in third-party public cloud services, it is often beneficial for an enterprise to have an on-premises server for many reasons. For more information, see this web page.

Running the IBM Blockchain Platform components outside of IBM Cloud provides you with more flexibility to grow or join a blockchain network. It also helps network initiators grow their networks by allowing new members to join while they use the platform of their choice. It allows organizations that are interested in joining blockchain networks to colocate their peers with their existing applications or to integrate with their systems of record.

Note: Users of this offering manage their own security and infrastructure. IBM Cloud does not provide those services.

Red Hat OpenShift Container Platform

Red Hat OpenShift Container Platform (OCP)[1] is a reliable and scalable cloud platform that can run on your on-premises infrastructure. It is built on open source frameworks, such as containers and Kubernetes. In addition, it offers common services for self-service deployment, monitoring, logging, and security, and a portfolio of middleware, data, and analytics with IBM Cloud Pak® solutions.

OCP on LinuxONE brings all of the benefits of reliability and scalability of Red Hat OpenShift, and provides excellent security without any changes in the application or containers. It also can scale vertically and horizontally, which helps process surges in workloads that occur because of any business environment changes (for example, a stock market surge that is the result of a catastrophic event).

For more information about Red Hat OpenShift and IBM Cloud Pak for LinuxONE at this web page.

[1] https://www.openshift.com/products/container-platform

Architecture overview of IBM Blockchain Platform for LinuxONE

Figure 5-2 shows a simple use case for IBM Blockchain Platform in IBM Cloud and IBM LinuxONE.

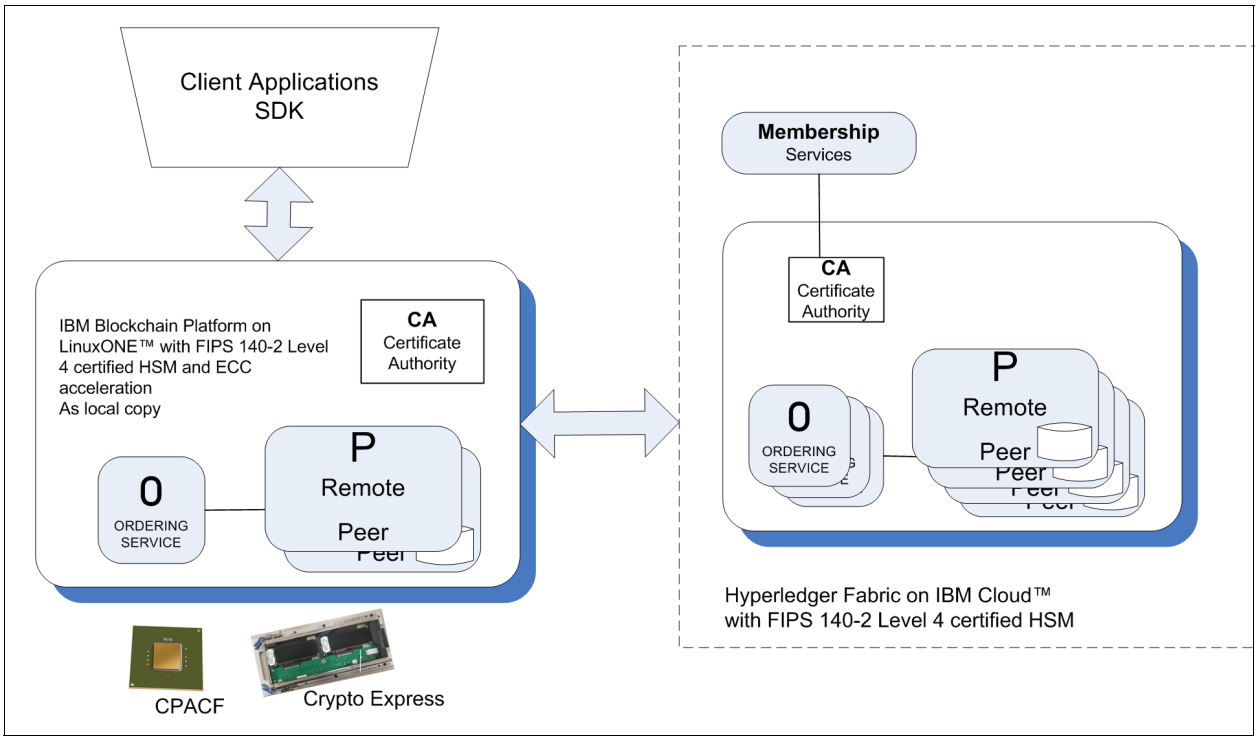


Figure 5-2 IBM Blockchain Platform for OCP use case

Supported features of IBP for Red Hat OCP on LinuxONE

At the time of this writing, IBM Blockchain Platform v2.1.3 for OCP supports Hyperledger Fabric v1.4.6 functions. This approach enables organizations to start building Hyperledger applications and test the connections to a main Hyperledger Fabric that is shared with other organizations. It also offers easy setup and integration to existing internal enterprise data stores. That way, you do not have to worry about making available data sets to an external cloud and about maintaining full control over the entire lifecycle of a blockchain network.

It can be deployed as a containerized service, working with selected Kubernetes management suites, such as Red Hat OpenShift. It also connects to various enterprise software suites, including IBM Cloud Pak.

For more information about the offerings on IBM Blockchain Platform for LinuxONE, see this web page.

How IBP for LinuxONE can use CPACF and Crypto Express security hardware features

IBM Blockchain Platform for IBM Cloud Private can use the cryptographic hardware that is built into LinuxONE. Starting with CP Assisted Cryptographic Functions (CPACF), when new blockchain data is generated, it uses a HASH function that is called (SHA-256) in CPACF. It then encrypts the data block in the file system with an AES block cipher, which also is in CPACF. IBP automatically uses these hardware features when used with supported Kubernetes platforms for LinuxONE.

LinuxONE can also be equipped with the Crypto Express co-processor feature, which is an HSM that is plugged into the PCI slot on the server. It meets the highest level of FIPS 140-2 standard, a level-4.

When equipped with Crypto Express co-processor, IBP can use protected key encryption for file systems. In this case, the encryption key for the block ciphers is always protected with another “key-encrypting-key” in the HSM. This function dramatically reduces the chance of exposing the encryption keys because it is protected by an HSM in the IBM Cloud and on IBM LinuxONE. In contrast, most of the other public cloud solutions store keys in memory as clear text.

The Crypto Express co-processor also helps accelerate blockchain processing times. It contains custom-built ASICs that accelerate asymmetric cryptographic functions, such as RSA or Elliptic Curve Cryptography (ECC). When encryption and authentication are required for blockchain processes, Crypto Express hardware can handle them much faster, compared to the use of only CPU cycles for the computations.

Hyperledger Fabric uses Elliptic Curve Digital Signature Authentication (ECDSA) for certificate authority enrollment and for encrypting blocks of data. Therefore, when you use ECDSA acceleration through an ECC unit in CPACF (LinuxONE III only), you can process more data in a shorter time. Its TCP/IP communications are also SSL/TLS enabled. Therefore, having RSA digital signature generation and verification helps to serve SSL/TLS traffic better with a Crypto Express co-processor.

For more information about HSM topics for IBM Blockchain Platform, see this web page.

A

Reference guide

Table A-1 lists some of the common cryptographic hardware libraries, tools, and drivers that can be used on LinuxONE.

Table A-1 Cryptographic hardware libraries, tools, and drivers

Name	Function
libcsulcca	The libcsulcca library provides APIs for CCA and secure key cryptography functions that are provided by cryptographic express coprocessor.
libica	The libica library provides hardware support for cryptographic functions. It is part of the openCryptoki project in GitHub. It is primarily used by OpenSSL through the IBM OpenSSL CA engine or by openCryptoki through the ICA token. A higher level of security can be achieved by using it through the PKCS #11 API implemented by openCryptoki.
openCryptoki	openCryptoki is an open source implementation of the Cryptoki API that is defined by the PKCS #11 Cryptographic Token Interface Standard. Therefore, openCryptoki supports several cryptographic algorithms according to the industry-wide PKCS #11 standards. The openCryptoki library loads the so-called tokens that provide hardware- or software-specific support for cryptographic functions.
z90crypt	z90crypt is a cryptographic device driver. It acts as the interface to the PCI cryptographic card coprocessor. This driver must be loaded to use CEX features.
zKVM	
virsh	You can create, delete, run, stop, and manage your virtual machines from the command line by using a tool that is called virsh. Virsh is useful for advanced Linux administrators who are interested in script or automating some aspects of managing their virtual machines.
qemu	Qemu is a machine emulator that can run operating systems and programs for one machine on a different machine. Mostly it is not used as emulator but as virtualizer in collaboration with KVM kernel components. In that case, it uses the virtualization technology of the hardware to virtualize guests.

libvirt	Although qemu has a command-line interface and a monitor to interact with running guests, it is rarely used that way for other means than development purposes. Libvirt provides an abstraction from specific versions and hypervisors and encapsulates some workarounds and best practices. libvirt is an open source API, daemon, and management tool for managing platform virtualization. It can be used to manage KVM, QEMU, and other virtualization technologies. These APIs are widely used in the orchestration layer of hypervisors in the development of a cloud-based solution.
vfio	The VFIO driver is an IOMMU/device-agnostic framework for making available direct device access to userspace in a secure, IOMMU-protected environment. That is, it allows safe, non-privileged, userspace drivers.
Linux tools	
`chzcrypt`	The **`chzcrypt`** command is used to configure cryptographic adapters that are managed by the cryptographic device driver and modify the AP bus attributes.
`lszcrypt`	The **`lszcrypt`** command is used to display information about cryptographic adapters that are managed by the cryptographic device driver and its AP bus attributes.
`icainfo`	The **`icainfo`** command is used to determine which libica functions are available on your Linux system.
`icastats`	The **`icastats`** command is used to determine whether libica uses hardware acceleration features or works with software fallbacks. icastats collects the statistical data per user and not per system.
`zcryptctl(KVM)`	The **`zcryptctl`** command is used to control access to AP queues and functions.
z/VM	

`QUERY CRYPTO`
 	
`DOMAINS USERS`
	These command queries can be used to show the status of the cryptographic hardware.
	
	When the DOMAINS operand is specified, the status of the installed AP domains is displayed. When the USERS operand is specified after the DOMAINS operand, the users who are authorized for CRYPTO APVIRT in the directory are listed.

REDP-5535-01

ISBN 0738458988

Printed in U.S.A.