

IBM Data Privacy Passports

*Pervasive data-centric protection
powered by IBM LinuxONE*



What is IBM Data Privacy Passports?

With the IBM LinuxONE™ III platform, IBM is addressing the privacy challenge with the cutting-edge Data Privacy Passports technology, which places LinuxONE at the center of your enterprise security. The ultimate goal to extend data protection and privacy from your LinuxONE environment to your entire enterprise is accomplished with this platform— in fact, extend it to wherever your data goes.

Instead of utilizing numerous solutions for data protection, you can use Data Privacy Passports, a consolidated data-centric audit and protection technology that protects data after it leaves the datacenter, minimizing the risk of security breach, noncompliance and financial liability.

This data security platform enables data to play an active role in its own protection and usage. With these capabilities, it enables you to achieve field-level data protection to protect that data throughout its lifecycle.

Benefits of data centric protection

Digital business risk is growing due to the challenge of maintaining control over data 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's critical to take measures to protect sensitive data at all times, even outside the limits of your datacenter.

The current standard of point-to-point encryption leaves many vulnerabilities and control risks for your data. Encryption and decryption occur through different siloed solutions at each location and in-flight as data traverses the enterprise network or is shared across hybrid multiclouds. This leads to lapses in data protection across hybrid environments and a lack of cohesive policy control for your data once it passes over to other

systems. According to recent research from Ponemon, 60 percent of companies have experienced a data breach caused by a third party.¹

With end-to-end data centric protection, data itself is encrypted at its starting point and remains encrypted until it reaches the endpoint. Data stored at endpoints and intermediate points maintain that encryption and the appropriate use of data is managed through centralized policy. Access and revocation can be managed regardless of where the data is located. This protection applies to IBM LinuxONE data as well as data from other platforms.

As a result, only the entitled application or user can view the data. This creates data protection that spans hybrid and multi-party computing environments, including data stored in public cloud deployments or shared with third parties.

Because of these benefits, Data Privacy Passports can help you:

- Meet regulatory and compliance mandates
- Minimize the enterprise risk and impact of collecting and storing sensitive data
- Control data sharing and usage on a need-to-know basis using a central control policy
- Manage compliance – track, monitor and report on how data is being used

What are the components of Data Privacy Passports?

There are 3 key components of Data Privacy Passports - Trusted Data Objects, Trust Authority, and Passport Controller.

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 with access and control is enforced through a centrally

¹ Opus & Ponemon, [Data Risk in the Third-Party Ecosystem](#), Nov 15, 2018

controlled policy in real time. A Trusted Data Object is the encrypted data element plus metadata. The data element is encrypted using a specific key (or set of keys) and all required instructions on how to process the Trusted Data Object are included in the metadata.

Trust Authority

The Trust Authority is where the policy governing the protection and usage of the data is maintained. The Trust Authority also serves as the main key store for the Data Privacy Passports solution. The Passport Controller communicates with the Trust Authority to obtain policy information and keys. An enterprise Trust Authority requires performant, scalable, and robust cryptographic and key management services making it an ideal match for LinuxONE.

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 gets clear data from a source DBMS and from there has several options to protect and enforce the data.

Our value proposition

Data Privacy Passports replaces point-to-point encryption and eliminates many vulnerabilities and control risks for your data.

Clients can implement field-level data protection without needing to make any changes to their applications and protect data throughout its lifecycle. This technology also enables clients to revoke access to field-level data that has left LinuxONE and provide fine-grained privacy control and consent management.

As the demand for privacy keeps growing, you can grow with it by expanding data protection beyond the enterprise. Help ensure that your enterprise data and client data are protected and private in today's open world with LinuxONE.

System requirements

In order to participate in the beta program for Data Privacy Passports, the following minimum system requirements are needed:

- IBM LinuxONE III
- IBM Crypto Express7S
- Db2® LUW
- Java™ Database Connectivity (JDBC) API
- Minimum 4 IFLs, 96GB memory, 128GB disk storage

How to move forward

Arrange a workshop to determine how deploying the Data Privacy Passports solution on IBM LinuxONE III infrastructure can improve your enterprise data protection and privacy.

Contact your IBM sales representative for additional details for the Data Privacy Passports beta program.

Evaluate the full IBM LinuxONE security and data serving portfolio by visiting these websites:

IBM LinuxONE III:

<https://www.ibm.com/marketplace/linuxone-iii>

IBM Data Privacy Passports:

<https://www.ibm.com/marketplace/data-privacy-passports>

© Copyright IBM Corporation 2019

IBM, ibm.com, IBM logo, Db2, LinuxONE and z/OS are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

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.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both. Other company, product and service names may be trademarks or service marks of others.

37027937-USEN-00

