IBM Data Privacy Passports

Pervasive data-centric protection powered by IBM Z

What is IBM Data Privacy Passports?

Pervasive encryption strengthened the security of IBM Z data since its introduction. But until now, you were unable to keep control over that protected data once it left the IBM Z® environment.

With the IBM z15™ platform, IBM is addressing that challenge with the Data Privacy Passports technology, which places IBM Z at the center of your enterprise security. The ultimate goal to extend data protection and privacy from your Z environment to your enterprise can be accomplished with this platform by setting appropriate policy levels. [2]

Instead of utilizing numerous solutions for data protection, you can use Data Privacy Passports, a consolidated data-centric audit and protection technology that has the capability to protect data after it leaves the system of record. By setting appropriate protection policy for your enterprise, users can reduce the risks associated from a security breach, and can help client address compliance requirements. [3]

This data security platform provides a data centric security solution that 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 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's critical to take measures to protect more than infrastructure – to protect sensitive data at all times, even outside the limits of your datacenter.

The current standard of point-to-point encryption can leave 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 is encrypted at its starting point and remains encrypted until it reaches the endpoint. Data stored at endpoints and intermediate points maintains 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. And this capability can be applied to IBM Z 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.

Because of these benefits, clients can use Data Privacy Passports to help them:

- With regulatory and compliance mandates [6]
- Reduce the enterprise risk and impact of collecting and storing sensitive data [4]
- Control data sharing and usage on a need-to-know basis using a central control policy [5]
- Manage compliance – track, monitor and report on how data is being used [6]

What are the components of Data Privacy Passports?

There are 2 key components of Data Privacy Passports -Trusted Data Objects and Passport Controller.

Trusted Data Object

A Trusted Data Object contains data that is protected and portable between multiple environments. A Trusted Data Object is the encrypted data element

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

[2] You can extend data protection and privacy for eligible data from your IBM z15 environment to your enterprise with Data Privacy Passports with appropriate policy controls.
Disclaimer: Data Privacy Passports supports data sources that can be accessed through a JDBC connection

[3]Data Privacy Passports on IBM Z is a consolidated data-centric audit and protection technology (DCAP) for eligible data that has the capability to protect data along its journey by setting appropriate data protection controls for your enterprise.
Disclaimer: Data Privacy Passports supports data sources that can be accessed through a JDBC connection

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.

Passport Controller

The Passport Controller is where the policy governing the protection and usage of the data is maintained. It also serves as the main key store for the Data Privacy Passports solution.

The Passport Controller is also the data broker that provides an intercept point to work in cooperation 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 a number of 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.[7]

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 IBM Z, 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 your enterprise keep its data protected and private in today's open world with z15.

System requirements

The following minimum system requirements are required:

- IBM z15 or IBM LinuxONE III
- An LPAR with either:
  - Four IBM IFL processors, 128 GB of memory, and 128 GB of disk storage, or
  - Eight IBM IFL processors, 256 GB of memory, and 256 GB of disk storage

IBM Data Privacy Passports requires Hyper Protect Virtual Servers V1.2 (5737-I09).

How to move forward

Data Privacy Passports solution on IBM z15 or LinuxONE III infrastructure can improve your enterprise data protection and privacy.

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

Evaluate the full IBM security software portfolio to create a layered security defense by visiting these websites:

IBM z15:
https://www.ibm.com/marketplace/z15

IBM Data Privacy Passports:
https://www.ibm.com/marketplace/data-privacy-passports

IBM Z Enterprise Security:
https://www.ibm.com/it-infrastructure/z/capabilities/enterprise-security

IBM Security Solutions:
https://www.ibm.com/security/solutions

[4] Data Privacy Passports is designed to help you reduce the risk and impact of collecting and storing sensitive eligible data in your enterprise
Disclaimer: Data Privacy Passports supports data sources that can be accessed through a JDBC connection

[5] Through a central control policy of Data Privacy Passports, you can control data access, sharing and use for eligible data.
Disclaimer: Data Privacy Passports supports data sources that can be accessed through a JDBC connection

[6] Data Privacy Passports can help you as you address your regulatory and compliance mandates by tracking, monitoring and reporting consumption of eligible data in your enterprise.
Disclaimer:Data Privacy Passports supports data sources that can be accessed through a JDBC connection

[7] Data Privacy Passports replaces point-to-point encryption for eligible data and is designed to reduce vulnerabilities and control risks for your data.
Disclaimer:
Data Privacy Passports supports data sources that can be accessed through a JDBC connection