IBM Z
FAQ
June 2020

IBM Data Privacy Passports

Frequently Asked Questions

Worldwide

Table of Contents

What is IBM Data Privacy Passports?

IBM Data Privacy Passports is a data centric audit and protection (DCAP) solution that protects and enforces appropriate use of data after it leaves the system of record, helping to reduce the risk of security breach and help clients meet their data compliance obligations.

What are the main functions of this offering?

Data Privacy Passports is a data centric security solution that enables eligible data to play an active role in its own protection. It lets you implement field level data protection to protect that data throughout its lifecycle.

The data protection policy is enforced from a central point of authority, the Passport Controller, that allows you to have control over your data, no matter where it later goes. As a result, only authorized applications or users can obtain a view of the data, where that view can be enforced through policy. This creates data protection that spans hybrid and multi-party computing environments, including data stored in public cloud deployments. Data can be protected on or off platform even in a hybrid cloud or public cloud; to open the encrypted data it must pass through the Passport Controller.

What is eligible data for Data Privacy Passports?

Data Privacy Passports only supports SQL structured data sources accessed via JDBC.

What is Protected data and Enforced data?

Protected Data

Protected data has been encrypted to help prevent unauthorized access by users who are not approved to view a given data element. A Passport Controller encrypts eligible raw data into protected data via Trusted Data Objects before leaving the platform. This protected data can be shown in different views based on the policy rules and the user's need to know. Note, the protected data could have a different schema and size.

Enforced Data

When an authorized user needs to view the protected data, the TDO must come back to the Passport Controller, which enforces the protected data by providing a view of the data that is appropriate for the requestor. That could be data in the clear, have a masked value, or hashed for a given user or application based on policy in the Passport Controller.

What are the components of Data Privacy Passports?

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

Trusted Data Object

A Trusted Data Object (TDO) contains data that is encrypted and portable between multiple environments. Data consumers can freely use eligible data from various sources while access and control is enforced through centrally controlled policy residing in the Passport Controller in real time.

A TDO is the encrypted data element plus metadata that are mathematically bound together. The data element is encrypted using a specific key (or set of keys) and all required instructions on how to process the TDO using the Passport Controller 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 and a data broker that transforms raw data into Trusted Data Objects. It also serves to enforce data protection policies.

The Passport Controller is deployed into a Hyper Protect Virtual Servers environment running on either IBM z15™ or IBM LinuxONE III. Note – The sources and target DBMS are not required to run on IBM Z® or LinuxONE servers. The Passport Controller supports structured data SQL data sources accessed via JDBC.

The Passport Controller gets raw data from source DBMS. There are then a few options:

1. Dynamic Enforcement – In this case the Passport Controller directly enforces the eligible data (according to the policy) coming from the source DBMS. In this case the Passport Controller intercepts the queries that would regularly be going to the source DBMS. There is no copy of the data.
2. Static Enforcement – In this case the Passport Controller is used to enforce eligible data from a source DBMS and save the contents into a target DBMS. The enforcement is done entirely based on the policy. Here there will potentially be several copies of data depending on the different enforcement that needs to be applied for different applications.
3. Protection – In this case the Passport Controller protects the eligible data (according to the policy) and stores the protected data (TDOs) into the target DBMS. Here there is a single copy of data saved as TDOs.

4. Protection and then Static or Dynamic enforce –In this case, the Passport Controller will be established as a proxy for accessing the protected table and will broker the SQL requests and apply enforcement to the data before it is returned to the consumer or it will create an enforced copy based off of the protected table. This is using a single copy of the data to provide multiple views.

Why is encryption first and enforcement second?

The order matters. This is because the policy may be defined in such a way that different personas (roles) are entitled to see different views of data. And it is possible to create a single protected table to be used in enforcing these different views of the data. This can be accomplished by protecting the eligible data first (creating TDOs) and then enforcing different views of the data when the data is consumed according to the policy through the Passport Controller. Enforcing the data first and then protecting it second could limit the options for enforcement at the point and time of consumption.

Who will encrypt the data? Who will insert data into a new table?

The eligible data will be encrypted by the Passport Controller to create a Trusted Data Object. When creating a Trusted Data Object (TDO) – data is encrypted and bound with metadata to create the TDO. The Passport Controller itself does not directly manipulate the source table. It transforms the raw data into TDOs according to the policy and then issues JDBC requests to create and populate the table into a target DBMS. The policy may be defined in such a way that some columns of a table are protected, and others are not. In this case, the row in the target table will contain columns that could be a mix of TDOs and "unprotected" data.

Is pervasive encryption mandatory for Data Privacy Passports?

Not mandatory, but complimentary. Data Privacy Passports does not require z/OS® data set encryption and z/OS data set encryption does not require Data Privacy Passports. While z/OS data set encryption is very effective at protecting data within the IBM Z environment, it does not protect data being moved off the IBM Z platform. Data Privacy Passports takes protection to the next level by adding protection to the eligible data as it is moved off the data source.

Pervasive encryption (z/OS data set encryption) and Data Privacy Passports can be used in combination. z/OS data set encryption can be used to protect the Db2® tables stored within the z/OS environment and Data Privacy Passports can be used to protect the eligible data moving off the platform (e.g. ETL). Remember, the data objects between the data source and the Passport Controller are not yet protected. The expectation is the data here would be protected in-flight via networks security protocols (e.g. TLS).

How does the encryption for Data Privacy Passports occur?

The Passport Controller encrypts the eligible data using AES 256-bit encryption keys. The target DBMS does not get keys for protected data (TDOs) they are stored within the Passport Controller. Access to protected data (TDOs) is brokered through the Passport Controller when the end user accesses the protected data through the Passport Controller.

Can customers run Data Privacy Passports on x86?

No. The security features that are the core of this offering are only available on the IBM Z platform.

Can customers run Data Privacy Passports in the cloud?

A cloud-based offering is not currently supported.

What is the role of the DBMS in this offering?

The Passport Controller must interact with the DBMS. On the source side, the data administrator will submit a combination of SQL requests and REST API calls to the Passport Controller. The SQL requests will be forwarded on to the DBMS. On the target side (protected table), the end users (e.g. data scientist, data owner, auditor) will initiate SQL requests for protected objects to the Passport Controller and the controller will forward these on to DBMS. Before returning the results of the query to the end user, the Passport Controller is designed to process the TDO and apply the policy to the data returned to the end user.

What databases are supported with this offering?

It is important to distinguish the difference between source DBMS and target DBMS. At the source DBMS the data administrator will interact with the Passport Controller to "ETL" the eligible data from the source to the target and apply either enforcement or protection as defined by the policy.

At the target DBMS, the Passport Controller will be established as a proxy to access protected data from the DBMS (The expectation is this proxy can be established without the end user knowing they are communicating with a proxy). Also, keep in mind enforced data or unprotected data can continue to be accessed directly from the target DMBS. It is important to realize that the Passport Controller does not internally contain a database, the data needs to be storage in an external target DBMS in the event that the data is enforced or protected via ETL.

What access methods are currently supported?

JDBC is the only data access mechanism supported. Many databases can be used and, in all cases, the required JDBC drivers need to be provided to the Passport Controller.

How do customers order this?

Contact your IBM sales representative for additional details.

What do I need to get started using this offering?

Contact your IBM sales representative for additional details.

Where can I find more information?

The following link has additional information:
https://www.ibm.com/marketplace/data-privacy-passports

®Copyright IBM Corporation 2020
IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.
Produced in the United States of America,
06/2020

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

The information contained in this documentation is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this documentation, it is provided “as is” without warranty of any kind, express or implied. In addition, this information is based on IBM’s current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this documentation or any other documentation. Nothing contained in this documentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM (or its suppliers or licensors), or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM’s sole discretion based on market opportunities or other factors and are not intended to be a commitment to future product or feature availability in any way.