IBM LinuxONE
Introduction
September 2019

IBM Data Privacy Passports

Frequently Asked Questions

Worldwide

28027928-USEN 00

IBM Data Privacy Passports

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, minimizing the risk of security breach, potential noncompliance and financial liability.

What are the main functions of this offering?

Data Privacy Passports is a data centric security solution that enables 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 that allows you to have full control over your data, no matter where it 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.

What is the relationship between Protected data and Enforced data?

Protected Data

Protected data has been encrypted to prevent unauthorized access by users who are not approved to view a given data element. A Passport Controller encrypts 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.

Enforced Data

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

What are the components of Data Privacy Passports?

There are 3 key components of Data Privacy Passports - Trust Authority, Passport Controller and Trusted Data Object. Let's look at each one.

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.

A TDO 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 TDO 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 IBM LinuxONE™.

For the initial delivery the Trust Authority and Passport Controller will be deployed together into a single Secure Service Container running on IBM LinuxONE III. Note – The sources and target DBMS are not required to run on LinuxONE servers. The initial delivery supports SQL data sources accessed via JDBC.

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 source DBMS from then there a few options:

1. Dynamic Enforcement – In this case the Passport Controller directly enforces the 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. Persisted Enforcement – In this case the Passport Controller is used to enforce 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 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. Protect and then enforce –In this case, the Passport Controller will be established as a proxy for accessing the protected table and will intercept the SQL requests and apply enforcement to the data before it is returned to the consumer. 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 data first (creating TDOs) and then enforcing different views of the data when the data is consumed according to the policy. Enforcing the data first and then protecting it second would 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 data will be encrypted by the Data Privacy Passport Controller. The Passport Controller encrypts data in two cases. At the data source when creating a Trusted Data Object (TDO) – Data is encrypted and bound with metadata to create the TDO. The controller itself does not directly manipulate the 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 a mix of TDOs and "unprotected" data.

How does the encryption for Data Privacy Passports occur?

The Passport Controller encrypts the data. Data Privacy Passports uses AES 256-bit encryption. The target DBMS does not get keys for protected data (TDOs). Access to protected data (TDOs) is brokered through the Passport Controller when the end user accesses the protected data through the Passport Controller. The Passport Controller communicates with the Trust Authority to obtain the key for a specific TDO.

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 @dp commands 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 will process the TDO and apply the policy to return enforced to the end user.

Why is Data Privacy Passports only available on LinuxONE III?

Data Privacy Passports is only being made available on LinuxONE III in order to be positioned for the combination of integrated compression and encryption capabilities available on LinuxONE III. When encrypting and protecting large amounts of data we want to ensure both compression and encryption are available in the hardware and the solution has access to the highest performing compression and encryption hardware.

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 LinuxONE platform.

Can customers run Data Privacy Passports in the cloud?

A cloud-based offering is not currently supported.

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 data from the source to the target and apply either enforcement or protected 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.

In the initial beta release, the supported source databases are IBM Db2® for z/OS®, Db2 LUW, IBM DVM, and Postgres. JDBC is the only data access mechanism supported in the initial deliverable. We are planning to add support for additional databases in future releases.

How do customers order this?

Contact your IBM sales representative for additional details. The beta service is available for free.

What is the roadmap and when will the service be Generally Available?

We are currently unable to offer any specific release date.

What are the pricing options?

Future pricing details will become available closer to the official GA release date.

What kind of support does IBM offer for this?

The beta service is an as-is offering, with no official support. There will be an official support option for the GA version.

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

IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.
09/2019

28027928USEN-00