Q&A Session for "IBM TechU Talk: Introducing IBM z15 Data Privacy Passports"

Session number: 926547468

Date: Thursday, April 9, 2020

Starting time: 10:25 AM (EDT)

Q: Are these features currently conceptual or available today?

A: It is available since March 20, 2020. The name of this product is IBM Data Privacy Passports (DPP).

Q: in this picture, the GA product is limited to the Private cloud square?

A: The solution runs on IBM z15 / LinuxONE III, but its services can be delivered to public/private cloud.

Q: DPP is a method of a centralized policy enforcer, or can it replace methods like Transport Layer Security (TLS), or do we need TLS and encryption technologies?

A: According to the policy, Data Privacy Passports (DPP) enforces data at the point of consumption (thanks to masking...), and protects the data at the point of exfiltration (thanks to encryption). As best practice, it is still needed to protect communications with TLS or similar alternatives.

Q: Can we dynamically refresh the trust credentials used between the endpoints without disruption to End-to-End (E2E) service?

A: If credentials are not trusted anymore, you have to update the policy. Or the External Identity Management shouldn't authenticate the user to allow DPP to deliver its services to this user as a requester.

Q: What is Hyper Protect?

A: Hyper Protect Virtual Server is a secured private cloud technology that runs on the IBM Z / LinuxONE. It provides highly secure virtual servers that can run Linux applications and containerized workloads.

Q: Since a Trusted Data Object (TDO) is created on IBM Z, can the data in it be accessed from other platforms (e.g., x86, Power)?

A: Yes, the TDO is created by Data Privacy Passports (DPP) for a defined target Database Management System (DBMS). The target DBMS processor architecture doesn't matter.

Q: Protected data: "this structure data source with JDBC connect..." on page 12. that is about the source; but the Trusted Data Object (TDO) is 'in-line' with the rest of the table in the target. And not all rows necessarily have a TDO associated, correct?

A: The TDO is a copy of the source from where the security of the data stays with the data. By the policy you can define what data will be encrypted as a TDO. Some data may stay in the clear. Nothing happens at the data source.

Q: Are Data Privacy Passports intended for Cloud application/platform, not just the z/OS level, correct?

A: Correct, IBM Data Privacy Passports enforces/protects data from data sources registered and known by DPP. This data sources may be running on IBM Z (z/OS or Linux on IBM Z), distributed platform, or in the Public Cloud.

Q: Is Db2 on z/VSE supported as a JDBC data source for Data Privacy Passports?

A: As long as Db2 on z/VSE support JDBC connection, it should work. If there is a specific JDBC driver for z/VSE you can upload via REST API in DPP so that it can be used with this DBMS.

Q: Can the Passport Controller run in a container extention (ZCX) under z/OS?

A: No, IBM Data Privacy Passports runs today in Hyper Protect Virtual Server.

Q: sFTP to a data lake? Data scientist using SQL queries?

A: DPP is able to push a Comma-Separated-Variable (CSV) file to a target system via sFTP. It can embed enforced data or protected data (TDO). To benefit of the Dynamic

Enforcement (experience of the data according the need-to-know) you have to SQL query DPP. It is not limited to data science.

Q: Does JDBC use DFM (Distributed File Manager)? Speaker mentioned DDM (which I assume is Distributed Data Manager). I thought that DFM on z/OS rarely is used. This implies that DFM will be used much more often. Is that true?

A. Speaker mentioned DVM (IBM Data Virtualization Manager for z/OS). This is a priced solution that facilitates access to both IBM Z relational and traditional non-relational data sources (eg. data sets). Supporting JDBC, it allows to be connected to IBM Data Privacy Passports, and so benefits its privacy services.

Q: In an enterprise we'd need more than one Passport Controller. Will you cover that, how data is synchronized between them, or can we load balance them etc...?

A: According to the use case, you may need multiple Data Privacy Passports instances and also Passport Controllers. IBM Data Privacy Passports itself do not store any data but keys, jdbc drivers and the policy. What has been encrypted by a Passport Controller can only be decrypted by this Passport Controller. In the future, architecture will evolve.

Q: Do you envisage we could have Passport Controllers in the IBM Cloud, thus enabling enforcement across organizations?

A: IBM Data Privacy Passports runs on IBM Z15 / LinuxONE III servers. The platform was chosen because its qualities of service--including robust security, reliability and availability as well as enterprise class scale and encryption performance --are closely aligned with the needs of the IBM Data Privacy Passports solution. Moving forward we do understand there are use cases that could be enabled by offering IBM Data Privacy Passports as a service.

Q: How does this relate to Data Privacy for Diagnostics?

A: It is not related directly to Data Privacy for Diagnostics, but both functionalities are part of the IBM z15 Privacy Journey.

Q: How do other platforms know how to work with the Passport Controller?

A: This requires a change in the SQL query route. Instead of SQL query the target DBMS, you have to SQL Query DPP that will execute and redirect the SQL Query to the target DBMS.

Output according the policy to be redacted according to the "need-to-know" of users. DPP plays the role of the man in the middle. You need to change the query route accordingly.

Q: Hi. How and where is the audit trace? Can we forward it to a SIEM?

A: Yes, there are tons of APIs you can consume (if allowed ;)). Output can feed ELK, Splunk, QRadar, or any SIEM-like solutions.

Q: Will we need Linux skills to install the Passport Controller?

A: Unix-like skills (such as Linux or MacOS command line), it is a matter of issuing specific commands.

Q: Will there be a follow up presentation about DPP that gets into the technical details of how to implement this?

A: IBM will probably have something at the TechU events scheduled for October 2020.

Q: I am Interested in more details about high-availability options for the passport controller / policy replication & synchronization across multiple controllers.

A. Thanks for the comment.

Q: Does this work with RACF controlled security for Db2?

A. Yes RACF and IBM Data Privacy Passports are complementary. RACF manages the authorization part, controlling who can access Db2 resources (users and IBM Data Privacy Passports application), while IBM Data Privacy Passports manages the privacy part, ensuring that the consumption to the Db2 data corresponds to the user's need-to-know.

Q: The Passport Controller seems like a "Single Point of Failure" (SPOF) for the whole system? If no access to Passport Controller, no access to any trusted data object?

A. IBM Data Privacy Passports v1.0 is designed to work as a stand alone solution. Moving beyond this initial design point, IBM recognizes the importance of evolving the IBM Data Privacy Passport solution to provide HA and DR capabilities. That said, one of the key reasons for deploying IBM Data Privacy Passports on LinuxONE or Linux on Z is the

robust reliability and availability provided by the server. Beyond this, one way to mitigate the risk is to use multiple passport controllers to segment source and target databases to reduce the impact of an outage caused by any one passport controller.

Q: Can a z/VM system be used to run the Linux on IBM Z needed for the Hyper Protect Servers, rather than natively in an LPAR?

A. Not at this time. IBM Data Privacy Passports must be deployed in an IBM Hyper Protect Virtual Server appliance running in an LPAR. z/VM is not part of the reference architecture regarding the deployment of IBM Data Privacy Passports.

Q: Does this work with RACF controlled security for Db2?

A: Yes, RACF controlled security for Db2 allows users to connect or not to Db2 (Security). Data Privacy Passports (DPP) will provide the appropriate experience of data according the user's need-to-know privacy level.

Q: Does the DPP install just like any other Secure Service Container (SSC) appliance?

A. Not exactly. DPP requires the installation first of Hyper Protect Virtual Server (HPVS) appliance, installed just like any other Secure Service Container (SSC) appliance. DPP is an application made of different components to be deployed as one inside a running HPVS appliance. That is the main difference.