Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS, Nidderdale House, Beckwith Knowle, Harrogate, HG3 1SA

Email: educationteam.ecs.uk@arrow.com
Phone: 0870 251 1000

IBM Data Privacy Passports

CODE:	LENGTH:	PRICE:
ESX3	16 Hours (2 days)	£1,300.00

Description

Data privacy is critical to you, but it has never been more challenging to maintain. Applications are spread across on-premises and cloud platforms, including sensitive data that needs to be protected everywhere. How can you protect your data after it leaves the system of record?

- Your sensitive data might already be protected with encryption on a trusted system of record, such as the IBM® Z. However, as soon as that data leaves the confines of the trusted system of record, several questions immediately come to mind:
- Can data privacy and protection be maintained and enforced?
- Your system of record is trusted to maintain data privacy and protection. When shared, sensitive data that was encrypted is decrypted, copied, and may or may not be reencrypted before it is stored. After it is taken from that system, data protections must remain intact. Adequate controls to retain end-to-end data privacy and protection must be available.
- Can access to data be revoked?
- Your sensitive data must always be protected, compliance must be guaranteed, and consent must be respected. If conditions that are related to your sensitive data change, such as access or use, the ability to respond and comply must be possible.
- Is data privacy and protection provable?
- Information about data access, use, and policies must be readily available for auditing purposes. In addition, time that is spent by your security staff, auditors, and developers to administer and prove proper data privacy and protection is in place, should be minimized.
- To help you safeguard your sensitive data and provide ease of auditability and control, IBM introduced a new capability for IBM Z® called IBM Data Privacy Passports. It can help minimize the risk and impact of data loss and privacy breaches when collecting and storing sensitive data. Data Privacy Passports can manage how data is shared securely through a central control of user access.
- Data Privacy Passports can protect data wherever it goes. Security policies are kept and honored whenever the data is accessed. Future data access may be revoked remotely via Data Privacy Passports, long after data leaves the system of record, and sensitive data may even be made unusable simply by destroying its encryption key.
- Data Privacy Passports is designed to help reduce the time that is spent by staff to protect data and ensure privacy throughout its lifecycle via a central point of control.

- IBM Data Privacy Passports extends your data security in several ways. This includes protecting sensitive data, even when it is shared over diverse environments, preventing unauthorized access, and enhancing data privacy within a trusted environment.

• This course will demonstrate how Data Privacy Passports will provide privacy protection to your environment and assist with your security strength in depth strategy.

• In this course you will learn how leveraging the Data Centric Audit and Protection (DCAP) capabilities of IBM Data Privacy Passports can help safeguard all sensitive data to comply with data privacy regulations, minimize the amount of sensitive data needlessly shared within the organization and to 3rd parties, ease the burden of manual and cumbersome audits, revoke access to sensitive data, and ultimately have full control over the protection of your data wherever it goes.

Important
This course consists of several independent modules. The modules, including the lab exercises, stand on their own and do not depend on any other content.

Exercises and recorded demos reinforce the concepts and technologies being covered in the lectures.

Objectives

After completing this course, you should be able to:
• Describe the DPP architecture: Policy, protection and enforcement
•You will be able to Design a DPP solution to protect data moving through the enterprise
•You will be able to explain the difference between Protected data versus Enforced data
•You will be able to describe the components Data Privacy Passports (DPP)
- Policy
- TDO
- Trust Authority
- Passport Controller
•You will be able to plan the resources required to setup DPP
•You will be able to configure and implement a DPP instance inside an HPVS LPAR
•You will be able to manage a DPP instance:
- Start and connect to your DPP instance
- Access your DPP controller and issue commands
- Manage keys
- Revoke Data Access
- Define and start a DPP policy
- Use DPP Programming interfaces: JDBC SQL REST APIs
-Work with TDOs: Source and Target DBMS

Audience

This class is intended for z/OS & Linux on z system programmers and IT specialists in charge of configuring, implementing and deploying DPP under z15.

Prerequisites

- General z15 and/or LinuxONE III architecture knowledge
- Basic knowledge of linux or linux on z
- Basic knowledge of linux command line interface (CLI)

Programme

Unit 1. Introduction to DPP and Data Privacy
•IBM Data Privacy Passports: The solution to Data Privacy
-Data Privacy
-Data Privacy Challenges
-Data Security and Data Privacy
-Data Centric Protection
-IBM z15: Data protection and privacy
-IBM Z: Pervasive Encryption
-Data Privacy Passports: Introduction
-IBM Z Data Privacy Passports Offering
-IBM Hyper Protect Virtual Servers
-Protecting data moving through the enterprise
-Protected data versus Enforced data
-What are the flows for enforcement on data
-Data Access Revocation
•DPP architecture: Policy, protection and enforcement
-Components of DPP
-Key components of IBM Data Privacy Passports
  -Policy
  -TDO
  -Trust Authority
  -Passport Controller
-Key Management

•Data Privacy Passports Use cases
•Data Privacy Passports: Designing your solution
•Useful Links and Resources
•Data Privacy Passports Resources

Unit 2. Installing and deploying DPP
•Planning for DPP
•DPP Deployment via HPVS

•Installation Prerequisites
•Data Privacy Passports Product Roadmap
•Configuring the HPVS LPAR
-Main Architecture overview and requirements
-Configuring the client
-package manager machine
-Package Manager Setup
-IBM Hyper Protect Virtual Servers download image
•Deploying the IBM Data Privacy Passports appliance in the HPVS Appliance.
-logon to the SSC Container web-UI
-configure network and disk storage
-DPP Appliance Deployment
-Create the DPP containers and quota groups
-Policy upload
-Testing that IBM Data Privacy Passports is successfully deployed
-TLS and LDAP configuration
•Configuring and using IBM Data Privacy Passports.
-use DPP REST APIs
-register and invoke an API
-Key creation
-Upload a policy
-Sign a policy
-Start a policy
-Manage keys
Unit 3. IBM Data Privacy Passport: Policy and Interfaces
-The DPP Policy
  -Design your sample policy
  -Users and groups
  -Policy Elements - Data Elements
  -Data Elements – Protection
  -Cryptographic Keys
  -Data Elements – Enforcement
  -Functional Roles & Groups
  -General Configuration Options
  -Defining Database Connections
  -Policy Management
-Data Privacy Passports: Programming interfaces
  -JDBC
  -SQL
  -REST APIs
  -REST API – Usage Patterns
Unit 4. IBM Data Privacy Passport: Data protection & Data enforcement
-Trusted Data Objects
  -Structure of Trusted Data Objects
  -Working with TDOs: Source and Target DBMS
  -Using Protected Tables
  -Static Enforcement
  -Dynamic Enforcement
  -Revocation of Protected Data
  -Recovery of Protected Data
-DPP policy: an example

Session Dates

On request. Please Contact Us

Additional Information

This training is also available as onsite training. Please contact us to find out more.