IBM Data Privacy Passports

Data-centric protection and privacy designed to safeguard your data wherever it goes

Highlights

- Protect eligible data as it leaves the source and travels across your enterprise[1]
- Help prevent unauthorized access to selected data with encryption, masking or hashing
- Simplify your compliance obligations with centralized access to policy controls
- Revoke future access to eligible data at any time

Digital business risk is growing due to the complexity of maintaining control over data that is increasing in volume, variety and value. Meanwhile, cyber attackers are finding increasingly innovative ways to compromise IT infrastructure and steal customer data, and regulators are authorized to impose fines on enterprises that don't properly secure it. Because of these risks, it is critical to take measures to protect sensitive data at all times.

Traditional security approaches often fail to protect data in today's digital business ecosystem. Many data protection solutions are siloed, focused either on protecting the network itself or the devices that access it. As data travels across platforms, different tools and techniques are used each time the data lands, which makes data protection difficult to manage and control. This can lead to lapses in data protection across hybrid multicloud environments and a lack of cohesive policy control for your data once it passes over to other systems. Security professionals must adopt an end-to-end data-centric approach to protect data as it moves from one platform to another.

IBM Data Privacy Passports is a data-centric audit and protection (DCAP) solution that protects eligible data after it leaves the system of record and moves throughout the enterprise and into distributed and hybrid cloud environments[1]. This allows authorized users to extract value from your data while helping to reduce the impact of security breaches to your organization.

DCAP solutions focus on the security of data itself rather than on the security of networks, hardware or software. Instead of utilizing numerous solutions for data protection, you can set appropriate protection policy for your enterprise to reduce the risks associated with a security breach and address compliance requirements. With end-to-end data-centric protection, once data is protected at its starting point, it remains protected. Data Privacy Passports replaces traditional point-to-point encryption and mitigates many vulnerabilities that could expose protected data to unauthorized users.

[1] Data protection benefits described in this document apply only to eligible data that passes through the Data Privacy Passports component known as the Passport Controller. Data Privacy Passports supports data sources that can be accessed through a JDBC connection or REST APIs.

Move protected data securely between environments

Now you can protect sensitive data and maintain privacy by policy as the data moves from its source throughout your enterprise—and across hybrid multicloud environments. Data Privacy Passports protects data sent to a REST API, or SQL structured data sources accessed via JDBC, and supports privacy of that data after it leaves the system of record. The Data Privacy Passports component known as the Passport Controller provides protection, enforcement, policy and key management for data that originates on IBM Z®, as well as data originating from other platforms once it passes through the Passport Controller.

Help prevent unauthorized access to eligible data using enforcement techniques

You can reduce the risk of sharing data by allowing your data to play an active role in its own protection, no matter where it travels. Protect data before it leaves the system of record by applying several enforcement techniques—including encryption, masking and hashing—to reveal only data that is authorized for a given user based on centralized policy controls that you define.

Data Privacy Passports provides two paths to convert data into a policy specified view using the Passport Controller as the data broker. The first method is to transform raw data into a Trusted Data Object, made up of the encrypted data element plus metadata. The data elements are encrypted using one specific key (or set of keys) and all required instructions on how to process the Trusted Data Object are included in the metadata. The second method is to create policy enforced views that determine at the point of consumption whether the field a user sees is clear or has an obfuscation technique applied to it. This method is useful in cases that cannot accommodate a change in schema and instead require a format preserved view.

Simplify your compliance with a centralized policy engine

The Passport Controller is where the policy governing the protection and usage of the data is maintained. It also serves as the key store for the Data Privacy Passports solution. At the point of data consumption, the policy active in the Passport Controller determines a user's entitlement to see data.

Centralizing access and control of your protected enterprise data across all platforms can help reduce cost and complexity[2]. Additionally, audit logs maintained by the Passport Controller track all activity within the data flow, providing a record of data access to assist with your compliance obligations.

Revoke future access dynamically

Traditional security solutions rely on trust-based protection rather than technical assurance to control appropriate access to data throughout its lifecycle. For instance, once a project comes to an end, there is no way to ensure that users who were authorized to access data for the purposes of that project will not access the data in the future.

Data Privacy Passports allows you to maintain control of your eligible data after it leaves the system of record and throughout its lifecycle. Once there is no longer a need to share data with a user, future access can be revoked at any time through dynamic policy updates or key destruction. With a policy update, you can change the way data fields are displayed for each user from that point forward. When a key is destroyed, all access to the Trusted Data Objects created with that key is removed.

[2] By reducing the cost of securing data and lowering the risk of a data or privacy breach, Data Privacy Passports are projected to deliver a five-year return on investment (ROI) of approximately 300%.
Disclaimer: Analysis based on a hypothetical ROI projection for IBM Data Privacy Passports, including the reduced risk of a data privacy breach, reduced risk of industry fines and regulatory penalties, policy enforcement efficiency and audit labor reduction, and the cost avoidance of an in-house equivalent implementation.

System Requirements

- IBM z15™, IBM z15 T02, IBM LinuxONE III or IBM LinuxONE III LT2
- 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 for deployment, which is built on the IBM Secure Service Container (SSC) framework.

Why IBM Data Privacy Passports?

Data Privacy Passports offers an end-to-end data-centric approach to replace point-to-point encryption for eligible data and helps eliminate many vulnerabilities and access control risks for your data. As the demand for privacy keeps growing, you can grow with it by expanding your data protection throughout your hybrid multicloud environment. IBM Data Privacy Passports is designed to help keep your organization's data protected and private in today's open world.

Why IBM?

The IBM z15 and IBM LinuxONE III platforms offer an industry-leading[3] level of security and resiliency across on premises, public and hybrid cloud environments.

Leveraged by businesses of all sizes, from large enterprises to next-gen startups, IBM Z and IBM LinuxONE represent a sound investment for your security solutions.

[3] The IBM z15 and IBM LinuxONE III platform Hardware Security Modules (HSM) provide FIPS 140-2 Security Level 4 cryptographic security, the highest level of security defined in this standard. At this security level, the physical security mechanisms provide a comprehensive envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access.

See https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Certificate/3410.

For more information

Contact your IBM sales representative for additional information on IBM Data Privacy Passports or call us, email us, or book a consultation by clicking “Let’s talk” on the IBM Z website.

Learn more about Data Privacy Passports:

- See how it works: https://www.ibm.com/support/z-content-solutions/data-privacy-passports/
- FAQ: https://www.ibm.com/downloads/cas/L8EWKEP9

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

- IBM z15: https://www.ibm.com/products/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