April 2020

IBM z15 Data Privacy Passports

Protecting data wherever it goes and generating a projected 335% ROI

An information security officer may sleep soundly knowing their organization's data is on an IBM Z®, encrypted at rest and in flight, with Pervasive Encryption protecting it from data loss. However, data must sometimes leave the Z, and that can be a concern. Once the data leaves the confines of a system of record, data loss is no longer the only problem. Privacy breaches become a possibility. However, a new Z capability, Data Privacy Passports, can guard against both data loss and privacy breaches with JDBC-addressable data sources. Data Privacy Passports can also provide a projected 335% return on investment over five years, with a seven month payback period, as described below.

Extending the value proposition of Pervasive Encryption beyond Z

At the time of this writing, Equifax had just announced a settlement of the federal, state, and consumer claims in the United States of at least US$650M.[1] The number may rise as it does not include unknown costs of credit monitoring for victims and other expenses. Much of Equifax's data was not encrypted. If it had been, the data loss could have been mitigated or avoided.[2]

With the launch of IBM z14® in 2017, IBM announced that its hardware was capable of such encryption while incurring a percentage increase in CPU utilization in the low single digits – on average, around 2.6%.[3] With faster encryption and on-chip compression in IBM z15™, that number is even lower.[4] The ability to encrypt data, both at rest and in flight, for a very low cost was welcome news for customers concerned about data security. Labeled "Pervasive Encryption", the capability eliminated many "non-functional" roles as potential threats of data loss. Non-functional roles are those that are not involved in the primary function of workloads running on the system. A storage administrator, for example, is such a role. The storage administrator needs to be able to move a database from one storage device to another but does not need access to the data inside the database. If the database is encrypted and the administrator has no access to the encryption key, that administrator cannot access the data.

However, in addition to data security, there is a question of data privacy. Data privacy considers functional roles and the minimum amount of data they require to perform their function, and what consent a data subject had provided to use their data. Within a system of record, interaction with data is constrained by applications. But, outside of that experience, data interaction is less structured. If a data scientist is looking at

---

[1] https://www.paymentsjournal.com/equifax-settles-credit-card-fines-hit-650-million-with-a-tail-that-could-run-4x/

[2] https://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Transcript-20171003.pdf

[3] https://ibmsystemsmag.com/IBM-Z/07/2019/z-os-data-set-encryption

[4] https://www.ibm.com/downloads/cas/AM1PYZBB

purchases all made by the same person, do they need to see the card number at all? In short, what does the functional role need to know to get the job done?

It is also important to keep in mind that these questions are answered at a particular time and place, and for a particular role. Rules change. Perhaps today it is permissible to display a full credit card number to a customer service agent, but tomorrow a new regulation requires that only the last four digits should be shown. Also, data moves. Credit card transactions are collected in an application running on IBM Z, but then sent elsewhere in an ETL (Extract, Transform, Load) cycle for analysis by data scientists, for example. Data must be protected wherever it goes and only what is required for a given role should be exposed given the most recent set of rules available.

In a typical data center, establishing and maintaining rules may require changing code in various applications, altering stored procedures, or even scrubbing over-exposed data and altering the ETL cycle.

Even if the movement of data is carefully tracked, the issue of data privacy represents a great deal of time and trouble, both of which boil down to expense. You could easily find yourself wishing that data could protect itself.

With IBM Data Privacy Passports, data from JDBC-addressable data sources can protect itself… and with far less time, trouble, and expense. This paper examines the potential benefits of a production-ready release of Data Privacy Passports.[5]

More than just encryption

An information security officer will have several concerns as data moves from a system of record, like a z15, out into the data center and beyond:

- **Data remains encrypted**. Encryption is at the heart of data protection. Data must remain encrypted in flight to its destination – a data lake perhaps – and it must be encrypted at rest there, as well.
- **Privacy is maintained**. Applications on a system of record are relied upon to maintain data privacy. Once taken from that system, privacy must remain intact. Proper controls to maintain privacy must be present.
- **Protection and privacy are provable.** Compliance must be assured, and audits must be straightforward.

Data privacy passports achieve this by creating “Trusted Data Objects”. A Trusted Data Object is an encrypted copy of the data along with security information about that data. When accessed, data in the Trusted Data Object passes through a Passport Controller.

[5] https://www.ibm.com/us-en/marketplace/data-privacy-passports/details

The Passport controller matches the identity of the requester to access policy and then may decrypt and transform the data. So, where a data owner may see a full credit card number, a data scientist may only see it masked. A central Passport controller, on the z15, implements and enforces policies. It also manages key material for the encryption and decryption of the data. As data is distributed and accessed, it may be in one of two states:

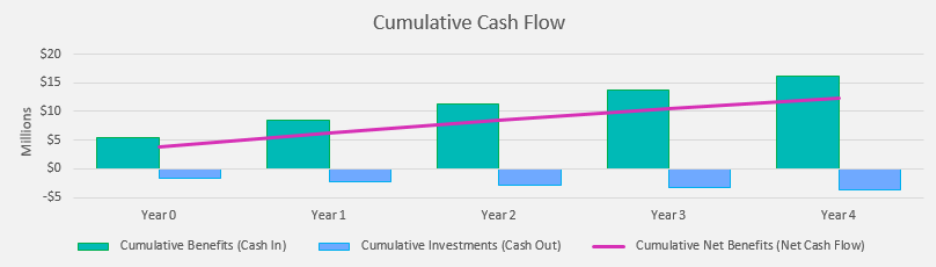
- **Protected** In this state, the original data is available if policy permits access in some form. It may be decrypted and transformed into an "enforced" state. In this state, it is a Trusted Data Object.
- **Enforced** In this state, data access policy has been enforced and the original data is not available. For example, a credit card number may be masked.

A great advantage of the Data Privacy Passports approach is that policy may be altered after data has been circulated. Because data passes through a Passport controller at the time of consumption, policy may be dynamic. A credit card number that was presented as four digits today may be completely masked tomorrow. Access to data can be revoked altogether by simply destroying the key required to decrypt it.

Another great advantage of Data Privacy Passports is that a significant return on investment can be achieved in less than a year.

A projected ROI of approximately 335% over 5 years

In a business value assessment of Data Privacy Passports, the IBM IT Economics team projects that a return on investment of between 310% and 360% may be achieved with a payback period of approximately seven months. Several factors are considered in this projection.



Projected cumulative cash flow from Data Privacy Passports, the parameters of which are detailed in this section

- Reducing the risk of data loss or privacy breach
- Avoiding the risk of industry fines and regulatory penalties
- Improving the efficiency of compliance policy enforcement and audits
- Avoiding the cost of an in-house implementation and maintenance of a similar solution

Reduced risk of data loss or a privacy breach

In calculating this benefit, we based our analysis on the average cost and likelihood of a data breach as reported by the Ponemon Institute in the report, "*Cost of a Data Breach Report 2019*", sponsored by IBM Security.

The financial risk of data loss or a privacy breach is calculated as the probability of a data privacy breach multiplied by the financial impact of a data privacy breach. So, for example, a 10% probability of a US$ 1 million problem is a US$ 100,000 risk. Data breaches vary in size – smaller breaches are more common than large ones. Our projection uses the annual likelihood of an average size breach: 9.6%.

In our data science example above, data in a data lake needs to be encrypted to prevent data loss, but there is also an opportunity for a privacy breach if information is improperly exposed to those with legitimate access to the data lake.

We asserted that Data Privacy Passports could lower the average likelihood of data loss or a privacy breach from 9.6% to 2%, or by a factor of 79%, which yielded a reduction in risk exposure of US$ 297,920 annually. We did not account for annual increases or fluctuations in probability or financial impact. We assumed that the average total cost of a data breach could be directly applied to data privacy breach, although we acknowledge the two are not the same.

Reduced risk of industry fines and regulatory penalties

Here, we calculated a potential industry fine or regulatory penalty of US$ 3 million based on a blended combination of penalties across several recent GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act of 1996), and PCI DSS (Payment Card Industry Data Security Standard) publicly disclosed violations. We calculated the average penalty per record and based our risk exposure on 27,901 records – an average size breach. We also assumed a 95% likelihood that an industry body or regulator would pursue a violation under normal circumstances. We posit that Data Privacy Passports could lower the average likelihood of an industry fine or regulatory penalty to 10%, or by a factor of 89%, based on eliminating the potential exposure of any Personally Identifiable Information (PII).

Compliance policy enforcement efficiency and audit labor reduction

By providing a single point of authority, Data Privacy Passports can lower the cost of managing data privacy policy compliance. It removes many points of potential failure – separate ETL transformations, access control lists, various native encryption options – and replaces them with one point of control and one point to audit.

In calculating this benefit, we assumed that 5 full-time equivalents (FTEs) would normally spend 25% of their time annually on data privacy policy compliance

enforcement. We posit that Data Privacy Passports could lower the time spent on compliance policy enforcement to 10% annual, or by a factor of 60% per FTE.

Its single point of authority also enables Data Privacy Passports to considerably lower the cost of data privacy compliance audits. In calculating this benefit, we assumed that 10 databases would need to be audited monthly, and that each database audit would normally take 8 hours to complete. We asserted that Data Privacy Passports could lower the time spent auditing each database 2 hours, or by a factor of 75%.

Cost avoidance of developing and maintaining an in-house solution

One also avoids the burden of cobbling together and maintaining an in-house solution. In calculating this benefit, we based our analysis on the assumption that an it would take approximately 17,280 person-hours, or a team of 12 FTEs 9 months to deliver a basic comparable solution. We assumed an average fully-burdened FTE hourly rate of $120. We did not make any attestation as to the function or quality of the in-house solution.

In addition to developing an in-house solution, we assumed it would take an average of 3 FTEs annually to maintain such an in-house based solution.

Bottom line: Data Privacy Passports are a great investment to reduce risk

Data Privacy Passports will protect data from JDBC-addressable data sources wherever it goes, reducing the risk of both data loss and privacy breaches. With Data Privacy Passports, security policy is maintained centrally, and it is honored whenever Trusted Data Objects are accessed, wherever they may have gone. Data access may be revoked after the fact, long after data has left the system of record. Data may even be destroyed simply by destroying its encryption key.

In addition to reducing risk, Data Privacy Passports reduces time spent by security staff, auditors, and developers protecting data. All of this combines to a significant return on investment.

About the authors

Mark Moore is a Senior Competitive Analyst and IBM Z Evangelist within the IBM IT Economics and Research team where he focuses on data security. Before joining the IT Economics and Research team he spent more than a decade as an IT Strategy consultant.

James Roca is an Executive IT Economics Consultant within the IBM IT Economics and Research team. James partners with IBM client CIOs / CTOs and their executive leadership teams to identify, evaluate, and define major enterprise-wide digital transformation programs that deliver tangible and long-lasting business value.

IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.
04/20

44027144-USEN-03