

IBM Z Security & Privacy - Technical

*Elevating protection for the data driven
enterprise*

—

Anthony Sofia (atsofia@us.ibm.com)
Senior Technical Staff Member, Master Inventor
IBM Z



Z

Extending IBM Z Security Leadership

Integrated Crypto HW

Massive secure transaction throughput

19xx



Encrypting Storage

Self encrypting tape and disk drives

2006



Pervasive Encryption

100% protection of IBM Z data within the system

2017



Quantum Safe Digital Signatures

Introduction of Crystals Dilithium digital signatures for secure audit logs (SMF)

Fibre Channel Endpoint Security

Ensure data integrity on the hardware level

2019

Data Privacy Passports

Data centric protection and enforcement on and off IBM Z

Data Privacy for Diagnostics

Serviceability without regulatory compromise



Manage huge growth of data with Pervasive Compression

Reduce data sizes by and improve workload execution time

Get started with compression now

Over 6x Compression ratio for storage savings, reduced bandwidth, faster transfer times

BSAM/QSAM compression saves space, elapsed time, and CPU.

Compression for file transfer: IBM Sterling Connect:Direct up to 80% reduction in file transfer time

Do more without limits

- Integrated Acceleration provides better reliability and eliminates complex planning and setup
- Standard on all IBM z15 processor cores - replacement for zEDC Express adapter
- Full Linux virtualization – 100% access for all LPARS and virtual machines
- No change to applications is required

Optimized Security with savings

Combine Pervasive Encryption with Integrated Acceleration for zEDC and get **optimized and secure** infrastructure

Save CPU and cost by combining compression with Pervasive Encryption

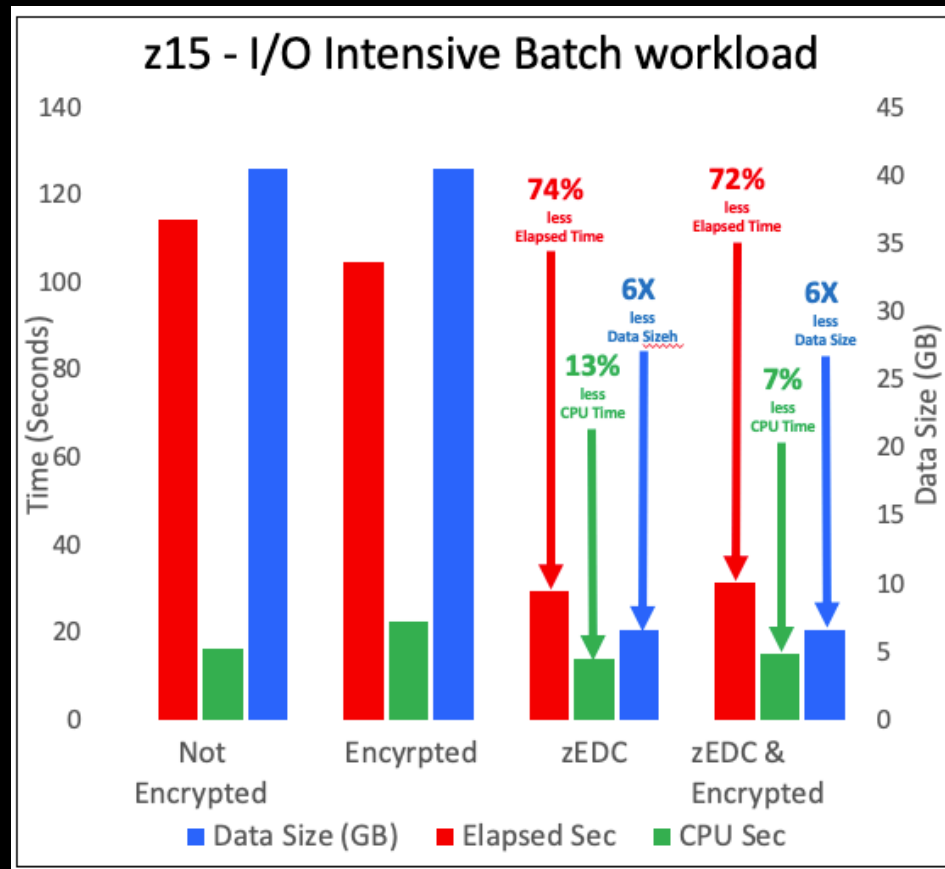
Pervasive Compression

Up to 17x more compression throughput than a max configured z14

zEDC - BSAM/QSAM dataset compression on z15

Integrated Accelerator for zEDC benefits on z15

- Using Integrated Accelerator for zEDC compression with BSAM/QSAM files on z15 can reduce file size by up to 83%, while improving CPU costs by up to 13% and elapsed times by up to 74% compared to using no compression.
- Integrated Accelerator for zEDC compression on z15 can reduce BSAM/QSAM file size by up to 6X compared to not using compression.
- Combining Integrated Accelerator for zEDC compression with BSAM/QSAM file encryption on z15 can improve elapsed time by up to 72% while reducing CPU by up to 7% compared to not using compression and encryption.



DISCLAIMER: Measurements completed in a controlled environment using a z/OS 2.3 batch workload accessing BSAM and QSAM sequential files. Results may vary by customer based on individual workload, configuration and software levels.

zEDC - BSAM/QSAM dataset compression on z15

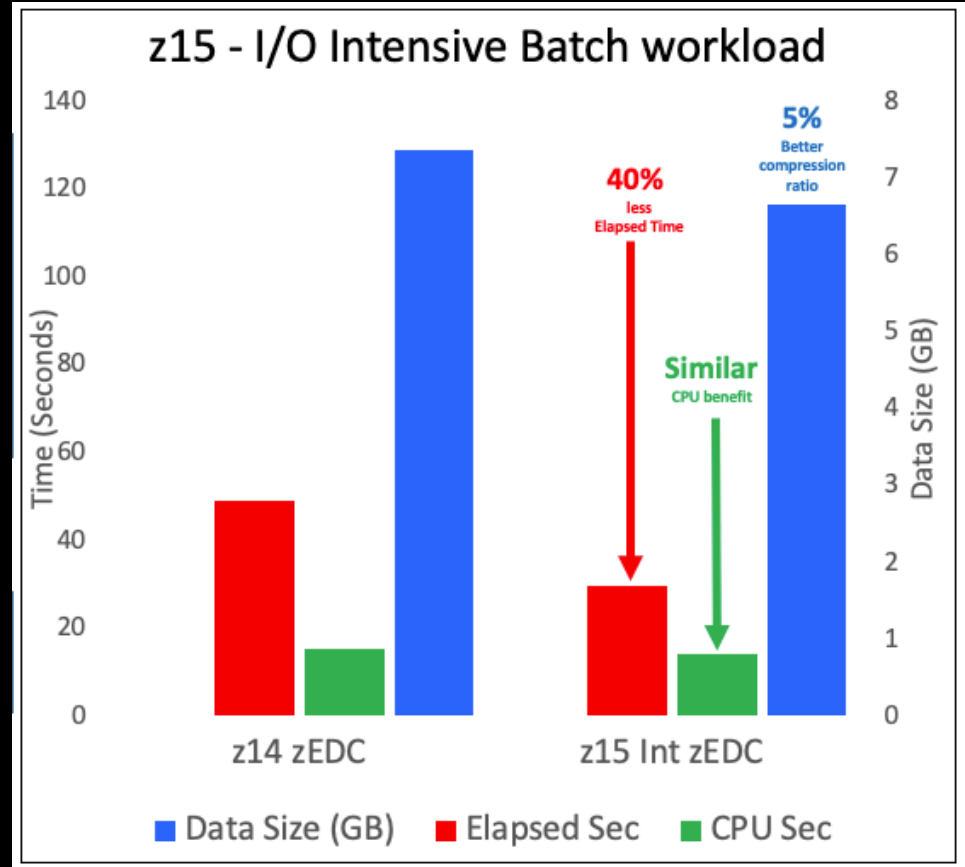
Integrated Accelerator for zEDC on z15 vs. zEDC on z14

- **Compressing BSAM/QSAM files with the Integrated Accelerator for zEDC on z15 improves batch elapsed times by up to 40% versus z14 zEDC Express.**
- **Compressing BSAM/QSAM files with the Integrated Accelerator for zEDC on z15 provides a CPU benefit which is similar to what is seen on z14 with zEDC Express**

DISCLAIMER: Measurements completed in a controlled environment. Results may vary by customer based on individual workload, configuration and software levels.

- **The Integrated Accelerator for zEDC on z15 improves the compression ratio by 5% over z14 zEDC Express.**

DISCLAIMER: Measurements completed in a controlled environment using a z/OS 2.3 batch workload accessing BSAM and QSAM sequential files. Results may vary by customer based on individual workload, configuration and software levels.



Extending IBM Z Security Leadership

Integrated Crypto HW

Massive secure transaction throughput

19xx



Encrypting Storage

Self encrypting tape and disk drives

2006



Pervasive Encryption

100% protection of IBM Z data within the system

2017



Quantum Safe Digital Signatures

Introduction of Crystals Dilithium digital signatures for secure audit logs (SMF)

Fibre Channel Endpoint Security

Ensure data integrity on the hardware level

2019

Data Privacy Passports

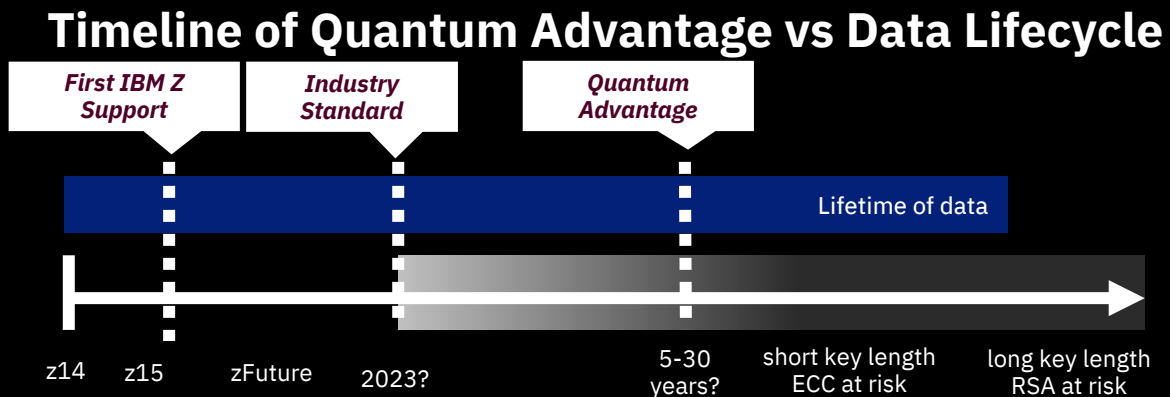
Data centric protection and enforcement on and off IBM Z

Data Privacy for Diagnostics

Serviceability without regulatory compromise



Next generation threats – Beginning the journey



Initial z15 Capability

Initially delivered via signing of SMF data to demonstrate

Agility in algorithms to update as standards evolve

Acceleration coming in HSM for essential primitives for Quantum Safe cryptography

Extending IBM Z Security Leadership

Integrated Crypto HW

Massive secure transaction throughput

19xx



Encrypting Storage

Self encrypting tape and disk drives

2006



Pervasive Encryption

100% protection of IBM Z data within the system

2017



Quantum Safe Digital Signatures

Introduction of Crystals Dilithium digital signatures for secure audit logs (SMF)

Fibre Channel Endpoint Security

Ensure data integrity on the hardware level

2019

Data Privacy Passports

Data centric protection and enforcement on and off IBM Z

Data Privacy for Diagnostics

Serviceability without regulatory compromise



End to end solution for data in flight protection

Future **IBM Fibre Channel Endpoint Security** to allow FICON or FCP Links from the z15 to the next generation of the IBM DS8000® storage family to be encrypted and protected

Statement of
Direction in
Announce – To be
delivered post GA

Challenges

- Corporate directive to encrypt all data in-flight.
- Ensure the integrity and confidentiality of data that is in-flight is protected.

Client Value

- Knowledge that all data flowing within and across datacenters are traveling between trusted entities
- Be able to provide auditable data verifying that customer data is only being accessed by trusted IBM Z and storage devices
- Supports all IBM Z operating systems
- Reduces and eliminates insider threats of unauthorized access to data in flight



Extending IBM Z Security Leadership

Integrated Crypto HW

Massive secure transaction throughput

19xx



Encrypting Storage

Self encrypting tape and disk drives

2006



Pervasive Encryption

100% protection of IBM Z data within the system

2017



Quantum Safe Digital Signatures

Introduction of Crystals Dilithium digital signatures for secure audit logs (SMF)

Fibre Channel Endpoint Security

Ensure data integrity on the hardware level

2019



Data Privacy Passports

Data centric protection and enforcement on and off IBM Z

Data Privacy for Diagnostics

Serviceability without regulatory compromise



Protection of data that must be shared

New **z/OS Data Privacy for Diagnostics** is a z/OS capability **exclusive to z15** with the ability to control access to data shared with business partners and eco-systems

Challenges

- Protection from accidentally sharing sensitive data when sending diagnostic information to vendors
- Concern for organizations who must comply with the GDPR laws and/or other data privacy laws and company mandates

Client Value

- Sensitive data tagging APIs combined with machine learning (ML) to detect, tag and redact all tagged data from diagnostic dumps
- MVP is working with 1st set of exploiters (Db2 and some DFSMS components) to provide the infrastructure to tag sensitive data in z/OS
- Tagging does not impact dump times
- Supported on IBM z15 running z/OS 2.3 or 2.4

IPCS - Post processor panel

```
----- IPCS MVS DUMP BATCH JOB OPTION MENU -----
OPTION  ===>

  1  SADUMP      - Prepare stand alone dump for analysis
  2  SVCDUMP    - Prepare SVC dump for analysis
  3  SYSMDUMP   - Prepare SYSMDUMP for analysis
  4  SUPPLEMENT - Perform supplementary dump analysis
  5  EREP       - Process software data using EREP
  6  DPFD      - Data Privacy for Diagnostics

JOB STATEMENT INFORMATION:  (Verify before proceeding)

===> //DPFD      JOB CLASS=C,MSGCLASS=A,TIME=1440
===>
===>
===>
===>
===>

Enter END to terminate batch job processing.
```

```
-----
*****
* USERID   - IBMUSER
* DATE     - 19/07/10
* JULIAN   - 19.191
* TIME     - 09:51
* PREFIX   - IBMUSER
* TERMINAL - 3278
* PF KEYS  - 12
*****
```

IPCS - Post processor panel

----- Data Privacy for Diagnostics Request -----

Press ENTER to edit parameters, END to terminate without job submission.

REQUESTED FUNCTION ==> ANALYZE (ANALYZE, REPORT, FEEDBACK, INGEST)

----- Data Privacy for Diagnostics Parameters -----

Press ENTER to submit the job, END to terminate without job submission.

COMMANI

```
DATA SET NAME          ==> 'SYS1.SDUMP.D190710.SV00009'  
NEW DATA SET NAME    ==> 'SYS1.SDUMP.D190710.SV00009.REDACTED'  
BYPASS DP ANALYSIS    ==> N          (Y or N)  
REDACTION STRING      ==> redacted          (0-32 characters)  
NUMBER OF THREADS     ==> 4          (1-4)  
ALLOW PAGE LEVEL      ==> Y          (Y or N)  
DPfD PATH             ==> /dpfdhome  
MIGLIB DATASET        ==> 'SYS1.MIGLIB'  
TEMP ALLOC PARMS     ==> UNIT(SYSALLDA)
```

Extending IBM Z Security Leadership

Integrated Crypto HW

Massive secure transaction throughput

19xx



Encrypting Storage

Self encrypting tape and disk drives

2006



Pervasive Encryption

100% protection of IBM Z data within the system

2017



Quantum Safe Digital Signatures

Introduction of Crystals Dilithium digital signatures for secure audit logs (SMF)

Fibre Channel Endpoint Security

Ensure data integrity on the hardware level



2019

Data Privacy Passports

Data centric protection and enforcement on and off IBM Z

Data Privacy for Diagnostics

Serviceability without regulatory compromise

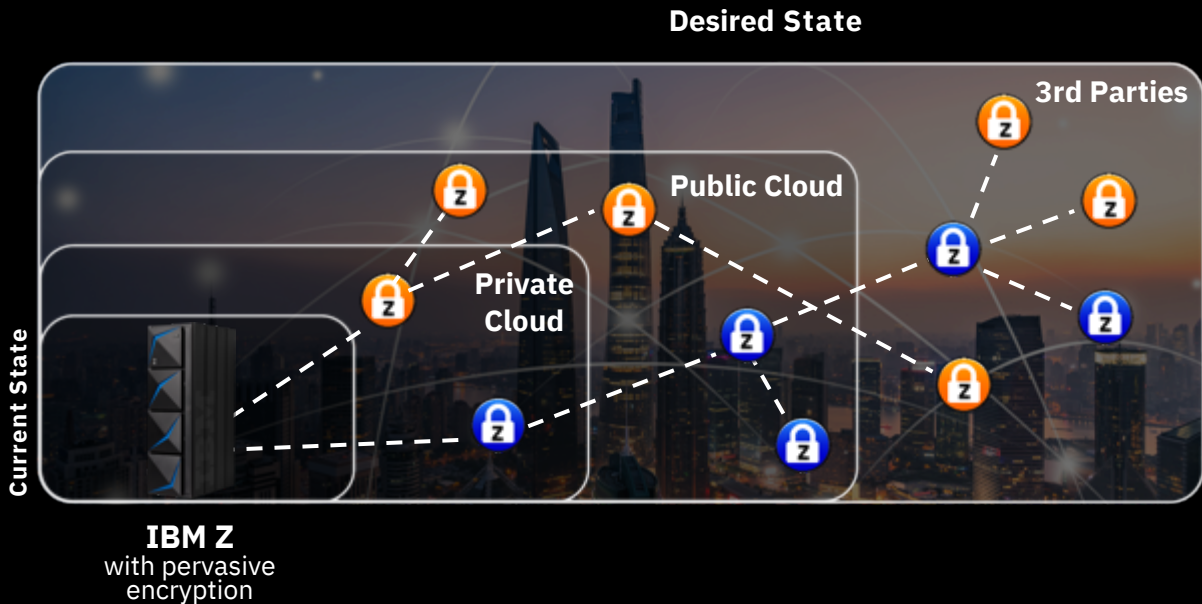


Protect individuals' identity in a digitized world

- **Protection** – Encryption and Revocation
- **Privacy** – Controls and Consent
- **Proof** – Audit and Compliance

\$40 to start an attack vector, \$40,000/HR for an attack recovery

-- Source: Eduard Kovacs, Security Week



| | |
|----------------------|---|
| Current State | Data protected within Z |
| Desired State | Data protected for the life of the data |

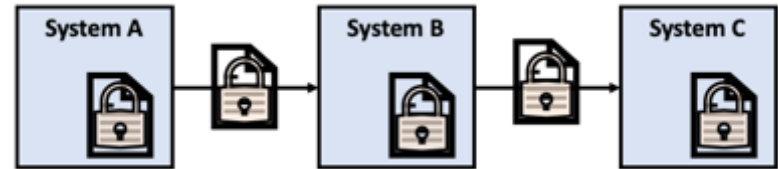
| | |
|--|---|
|  Desired State: Trusted Data Objects | <i>End-to-end protection via "Trusted Data Objects"</i> |
|  Desired State: Enforced Data | <i>Controlling the usage of data and auditability of data</i> |

Data Centric Audit and Protection (DCAP)



point-to-point

data is protected via encrypted network sessions. encryption & decryption occurs at each point as data traverses the network. any data stored at endpoints and intermediate points must be explicitly encrypted.



end-to-end

data itself is encrypted at the starting point and remains encrypted until it reaches the end point. data stored at endpoints and intermediate points is implicitly encrypted and managed through centralized policy

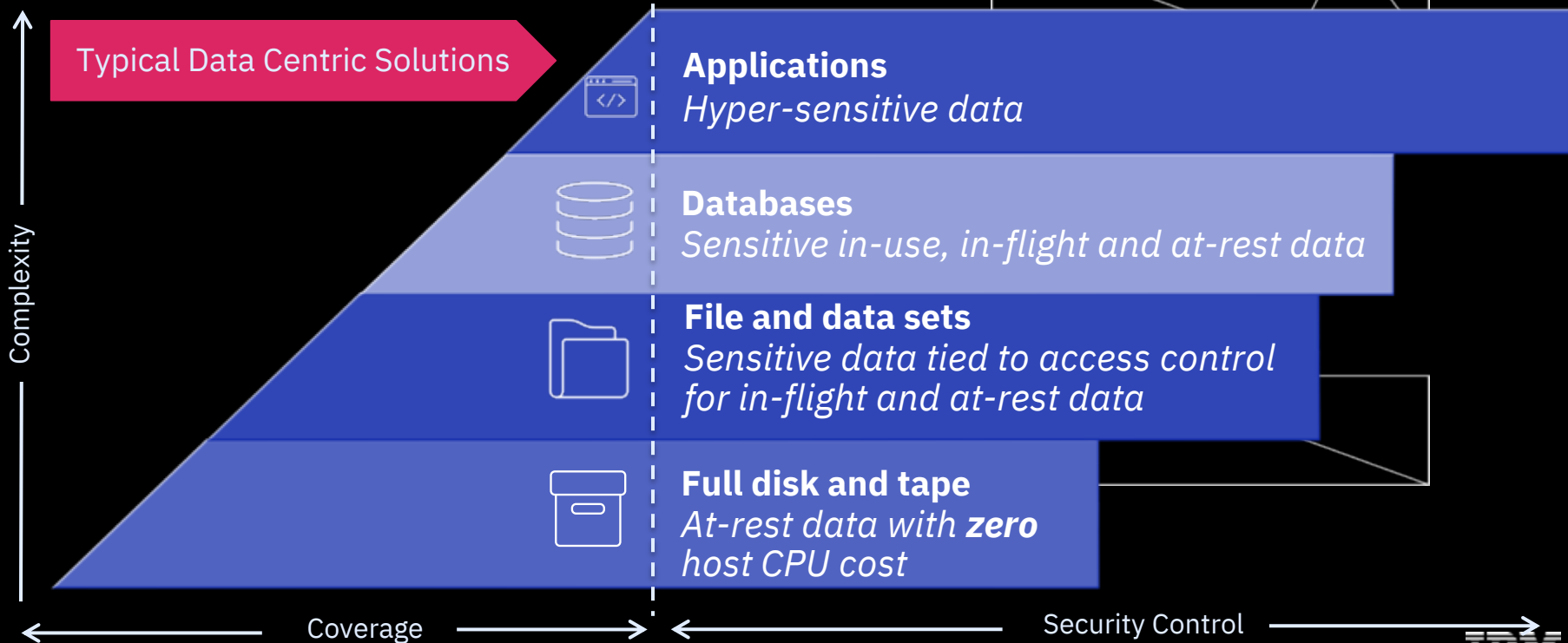
Extending Pervasive Encryption value

e.g. TLS, AT-TLS, IPsec,
MQ AMS, Connect: Direct Secure Plus,
Encryption Facility, SFTP, etc...

Smart, Secure Data Movement
Application transparent protection
for data leaving IBM Z

Achieving Data Centric Protection

- Typical application level protection is extremely costly and only protects a small number of fields
- Can you have security control with broader coverage and less complexity?

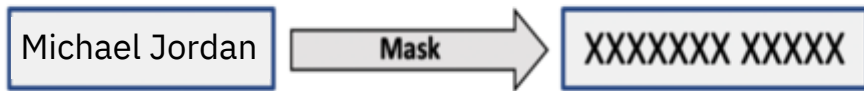


IBM Z Data Privacy Passports Offering

- Provides protection and enforcement for IBM Z data on **and off** the platform
- Complements Pervasive Encryption
- Data protected by Pervasive Encryption still needs this next level of protection

Protected Data (reversible)


- Data elements are encrypted into
- Trust Data Objects before leaving the platform
- Data can be shown in different views based on the user's need to know



Enforced Data (irreversible)

- Data elements are transformed (masked, encrypted, hash, omitted) at the time of consumption
- Transformations based on a user's need to know
- Can be performed on Protected Data or "on the fly"

What are the flows for enforcement on data



Data can be enforced “on the fly”

- Source data remain in the clear and clients connect to a proxy which will enforce data for them
- No changes needed to the database system where the data originates

Data can be protected then enforced

- Source data is encrypted into Trust Data Objects (TDO) and then inserted into a new table
- Clients connect to the new protected table and based on policy are presented an enforced view of the data
- The new protected table elements are stored encrypted

Where is the protected or enforced data stored

Enforced Data

- Can be stored in a table with the same schema as the source table
- Data can be enforced in a way where it remains compatible with the original source schema
- Easy for application transparent enforcement

Protected Data

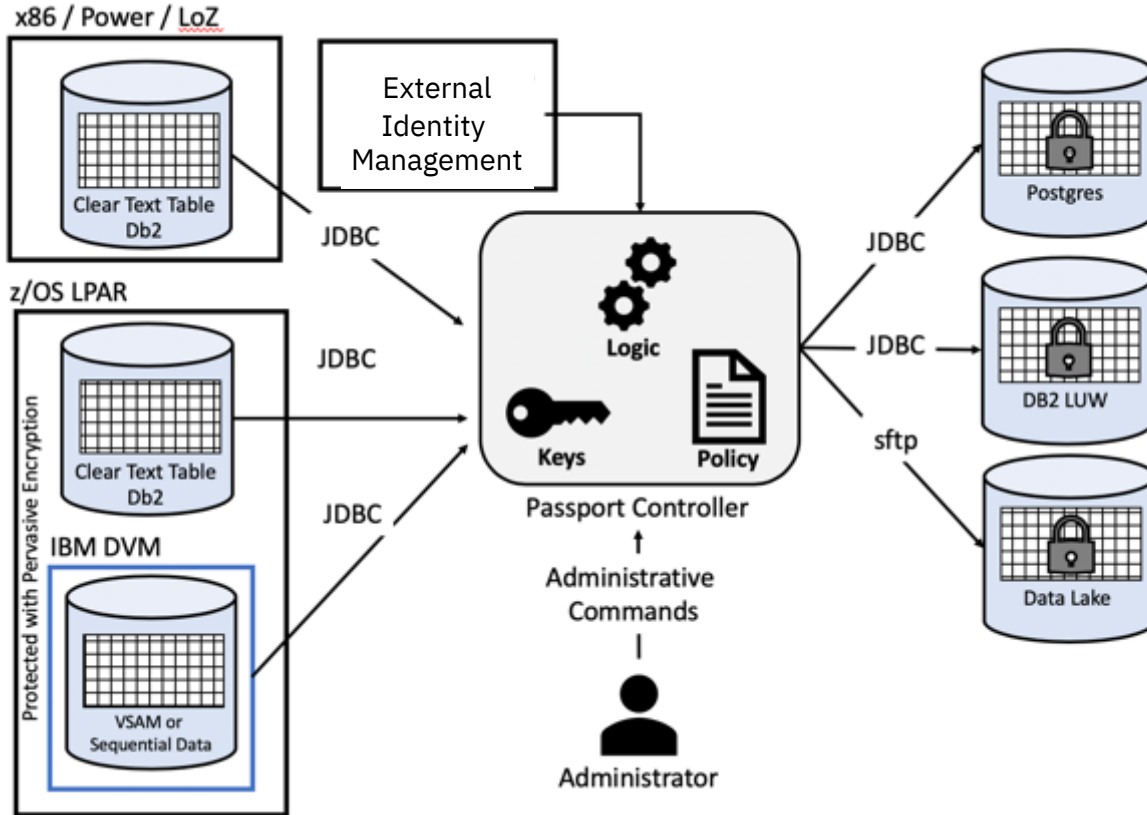
- Data elements can be packaged into Trust Data Objects (TDO)
- The TDOs do not share the same size as the source data, it is an encrypted package with additional metadata
- The target tables needs to be able to store data with a different schema than the source table
- This table can be on any system and does not need to be managed by the same database as the original source table

Minimal Viable Product Deployment

Passport Controller with Integrated Trust Authority

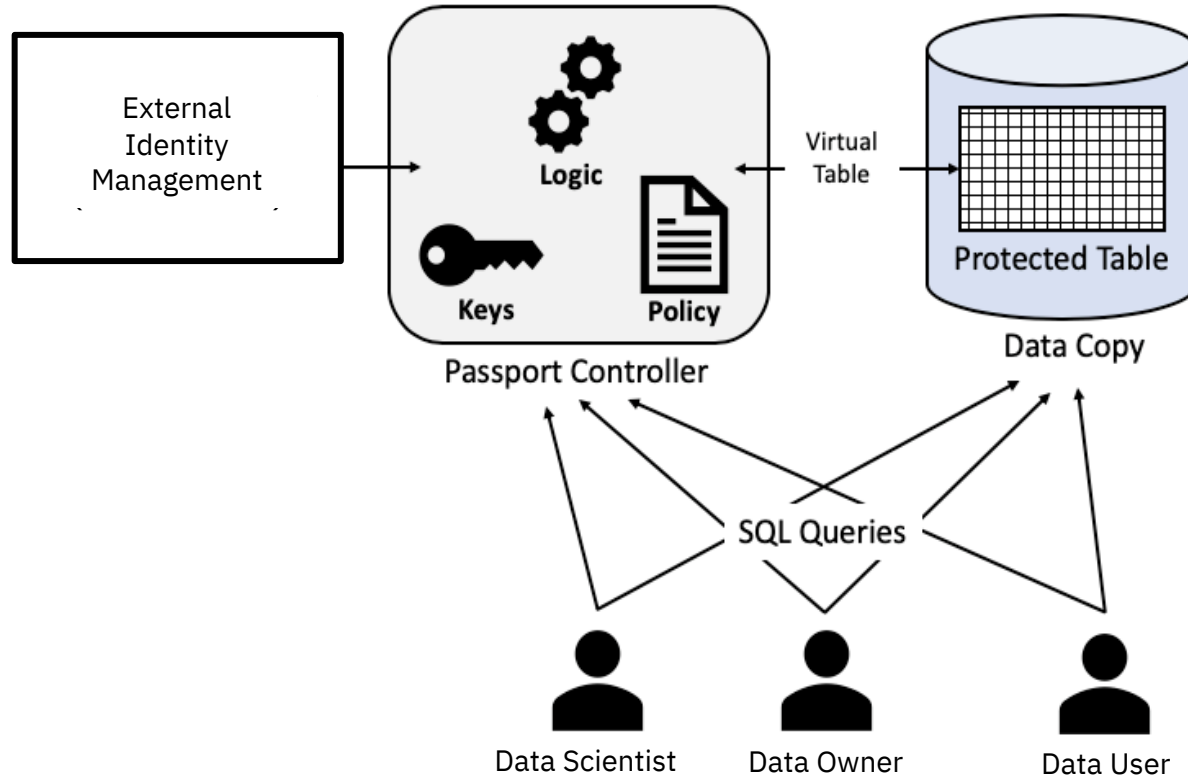
- Passport Controller and Trust Authority will be combined for easy deployment
- Simpler on-ramp for first set of use-cases
- Deployed in an SSC LPAR
- Manual policy management
- **All data access through controller is audited**

Protect IBM Z Data In the Enterprise (ETL)



- The data is protected at the point of extraction and is enforced at the point of consumption
- Move data from IBM Z to distributed as Trusted Data Objects – Start with SQL data sources on IBM Z
- Passport Controller deployed in an SSC LPAR
- **Create a single protected table to provide multiple views of data**

Use IBM Z Data In the Enterprise (ETL)



- Enforce data on distributed platform using Passport Controller on IBM Z at the time of consumption
- Identity can be managed on IBM Z (i.e. z/OS)
- Policy for enforcement can be changed dynamically to revoke to entitle users to data
- Connection to Passport Controller through industry standard Apache Hive drivers

Single Source of Protected Data

Create a single protected table from a policy on Z that allows multiple views of data from a single data source

Data Lake



Data Scientist

| first_name | last_name | s_num | phone | zip_code |
|------------|-----------|-----------|----------------|----------|
| Brian | Acosta | 999999999 | 669 706 2691 | 36593 |
| William | Adams | 999999999 | (710) 105-9539 | 12575 |
| ... | ... | ... | ... | ... |



PHONE and ZIP_CODE values are unencrypted and displayed as a one-time masked value

Data Owner

| first_name | last_name | s_num | phone | zip_code |
|------------|-----------|-----------|----------------|----------|
| Brian | Acosta | 128967796 | 669 208 1483 | 94016 |
| William | Adams | 409791779 | (710) 637-0338 | 94131 |
| ... | ... | ... | ... | ... |



ALL protected fields are unencrypted and displayed

Data User

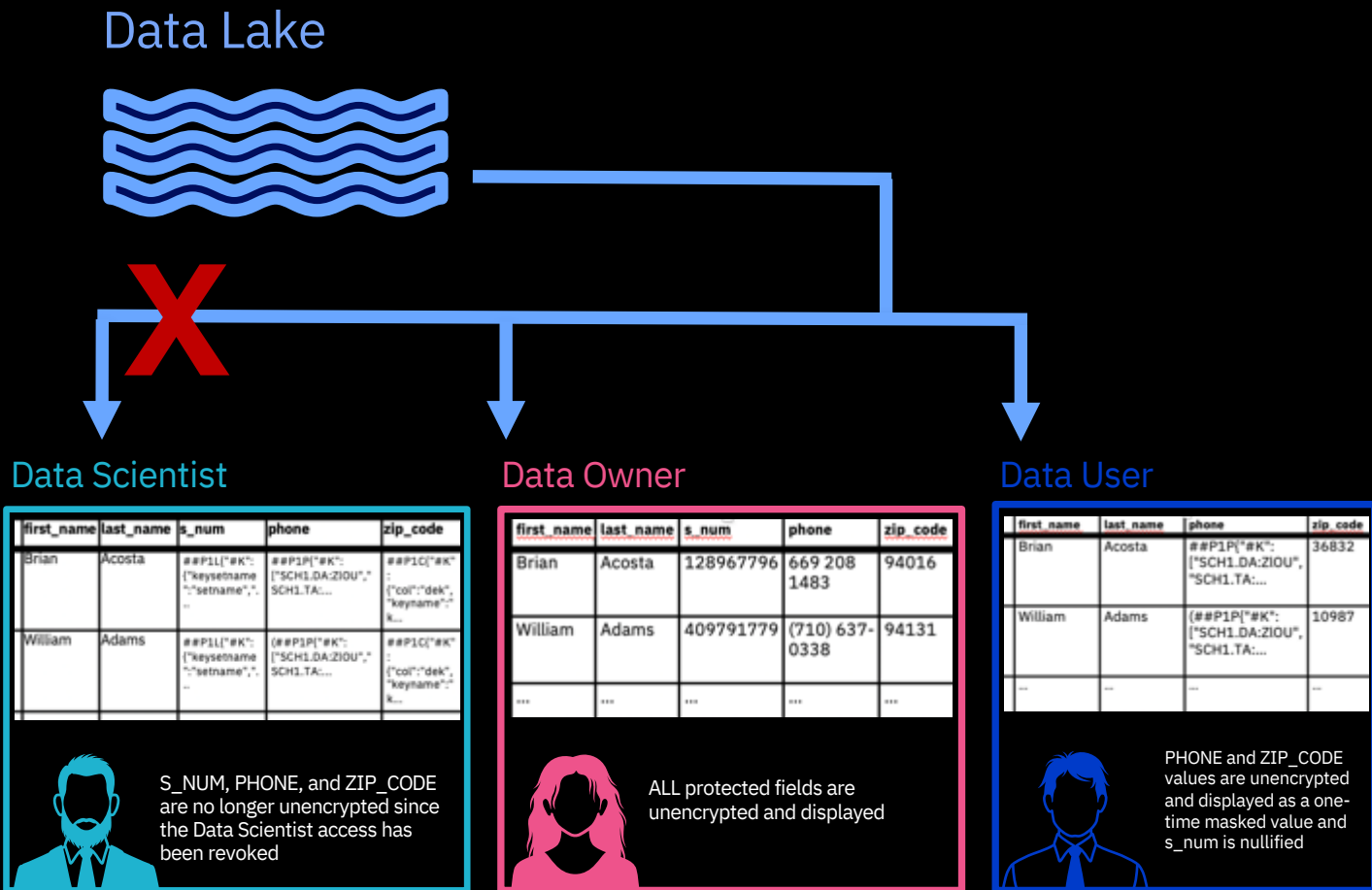
| first_name | last_name | phone | zip_code |
|------------|-----------|--|----------|
| Brian | Acosta | ##P1P["#K": ["SCH1.DA:ZIOU", "SCH1.TA:..."] | 36832 |
| William | Adams | (##P1P["#K": ["SCH1.DA:ZIOU", "SCH1.TA:..."] | 10987 |
| ... | ... | ... | ... |



PHONE and ZIP_CODE values are unencrypted and displayed as a one-time masked value and s_num is nullified

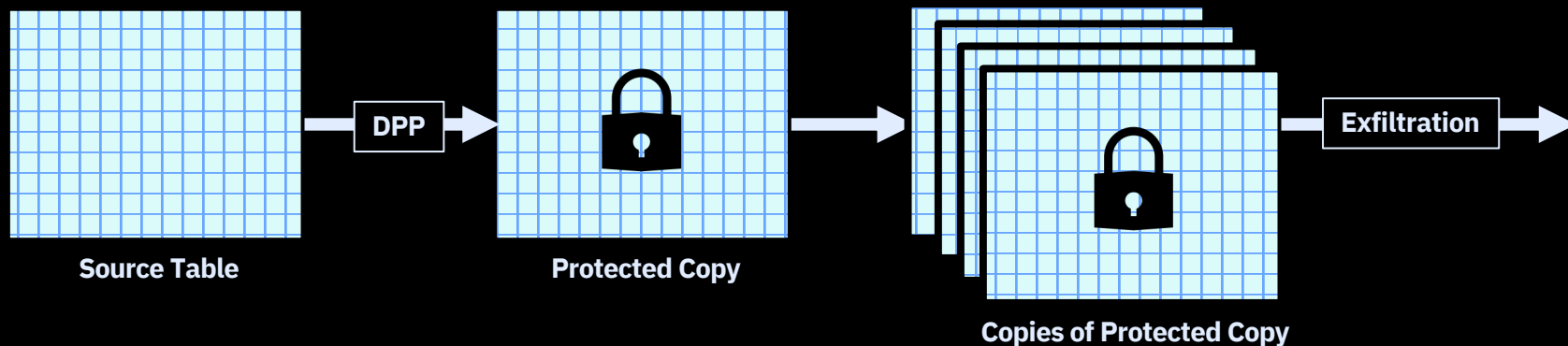
Revoke Access Remotely

Policy for enforcement can be changed dynamically to revoke to entitle users to data



Protecting Copies of Copies of Copies ... of Copies

- Utilize the basic principle of data centric protection
- Protect Personally Identifiable Information (PII) as it leaves IBM Z by policy
- All copies retain protection
- Opening the data requires a return trip to the **Passport Controller**



Data Access Revocation

Dynamically revoke access to data for specific users or all users



Policy Updates

- Users can be dynamically included to excluded from Trust Zones (groups) which have access to open Trusted Data Objects
- When a user is excluded from a Trust Zone, the Passport Controller will return the Trusted Data Object on a query rather than an enforced view
- Allows some users to continue to access data

Key Destruction

- Applies to Trusted Data Objects protected with an administrator generated key
- The key is deleted, which causes the Passport Controller to not open any Trusted Data Objects
- Applies to all users of the Trusted Data Objects, no users will have access

IBM Z Data Privacy Passports - Protected, Private, Provable



- Create a single protected table to provide multiple views of data
- The data is protected at the point of extraction and is enforced at the point of consumption
- Move data from IBM Z to distributed as Trusted Data Objects or Enforced data
- Tracks the complete data transformation journey from point of origin to consumption
- Policy access can be changed dynamically to revoke or entitle users access to data

IBM