IBM WW Z Security Conference

October 6-9, 2020

IBM Data Privacy Passports in action !

Guillaume Hoareau

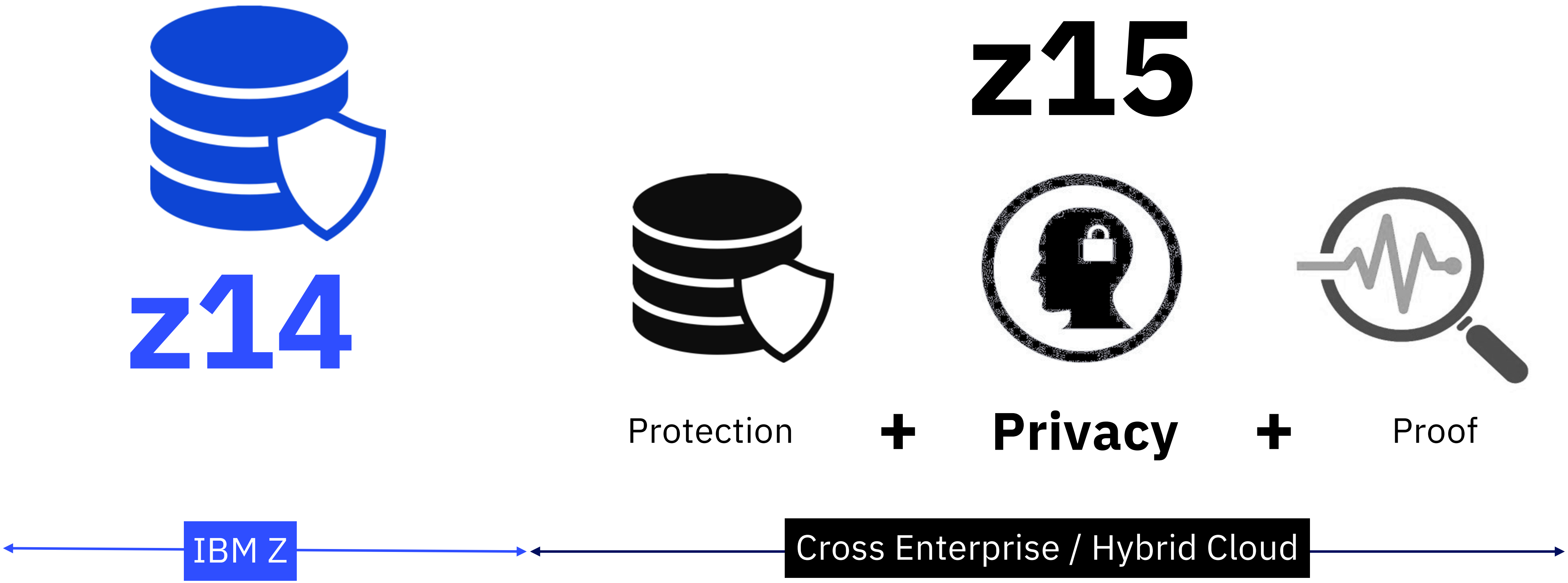
Certified IT Architect, IBM Systems Lab Services, Europe

guillaume_hoareau@fr.ibm.com

Agenda

- **Rapid introduction of IBM Data Privacy Passports**
- IBM Data Privacy Passports in action

IBM Z Security



z14

z15

Protection + **Privacy** + Proof

IBM Z

Cross Enterprise / Hybrid Cloud

Data Security Vs. Data Privacy

Data Security

Keeping data safe

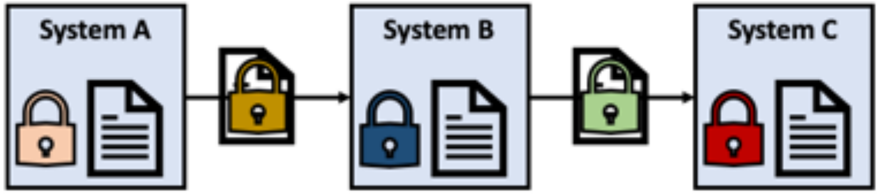
“Need-to-Access”

Data Privacy

Appropriate use of data

“Need-to-Know”, “Need-to-Share”

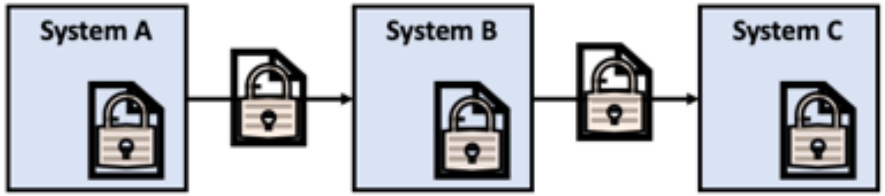
Data Centric Audit and Protection (DCAP)



Siloed (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.

E.g. TLS, AT-TLS, IPSec,
MQ AMS, Connect: Direct Secure Plus,
Encryption Facility, SFTP, etc…



E2E (End-to-End)

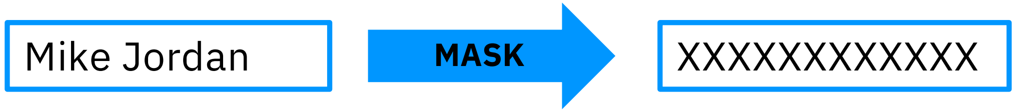
- Data itself is encrypted at the starting point and remains encrypted until it reaches the end point.
- Data stored at endpoints and intermediate points is implicitly encrypted and managed through centralized policy.

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

IBM Data Privacy Passports **enforces** and **protects** data

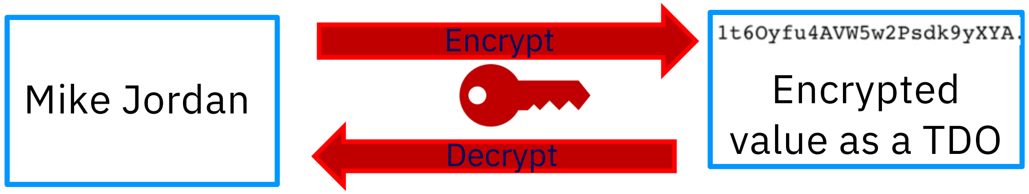
Data Enforcement – Irreversible* --

- Data elements are transformed (Masked, Encrypted, Hash, Omitted, Absorbed, Truncated…) at the time of consumption
- Transformations based on a user's "need to know" defined in the policy.
- Can be performed "on the fly" or to generate a "persistent" enforced table.



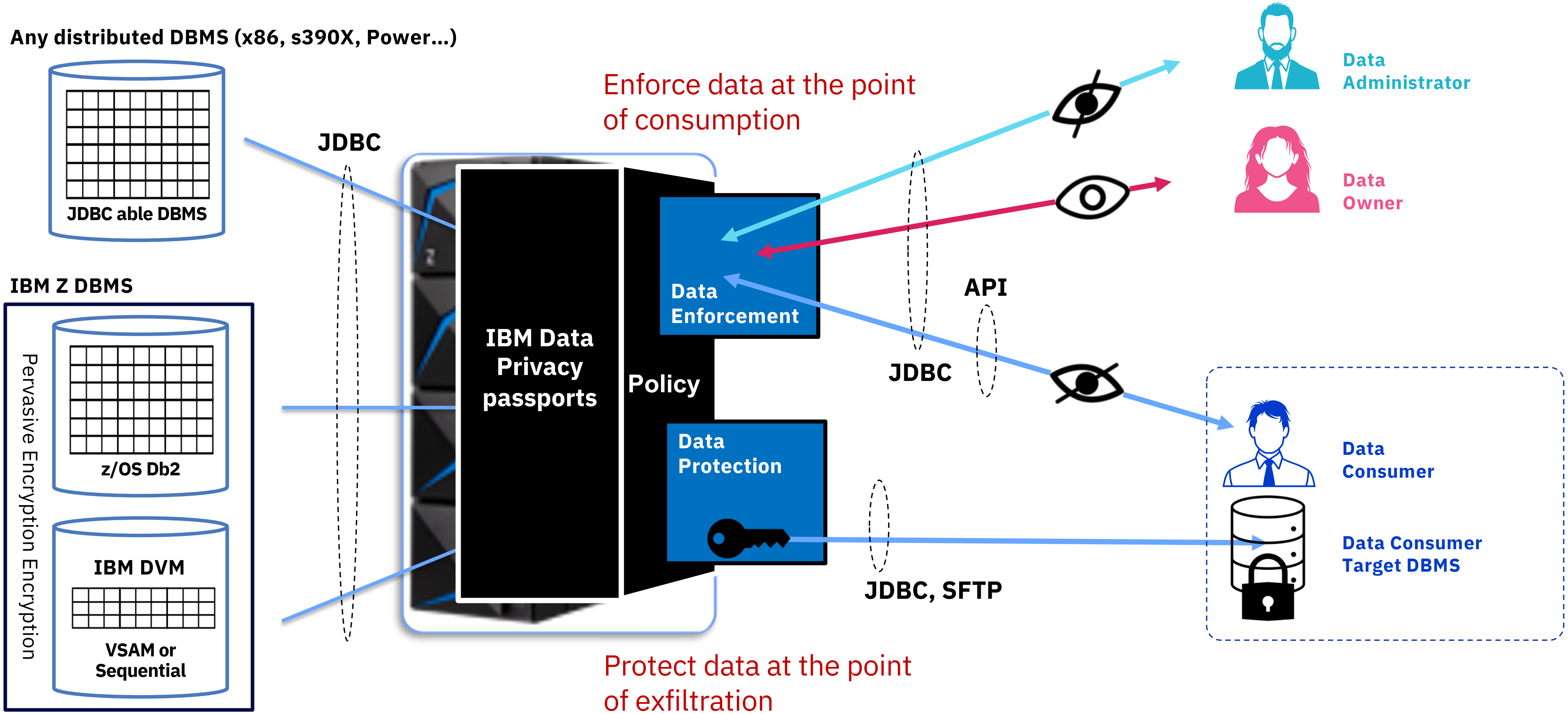
Data Protection -- Reversible --

- Data elements are encrypted into Trust Data Objects before leaving the platform.
- Transformations based on a target group's "need to know" rules defined in the policy.
- Data can be shown in different views based on the user's need-to-know.

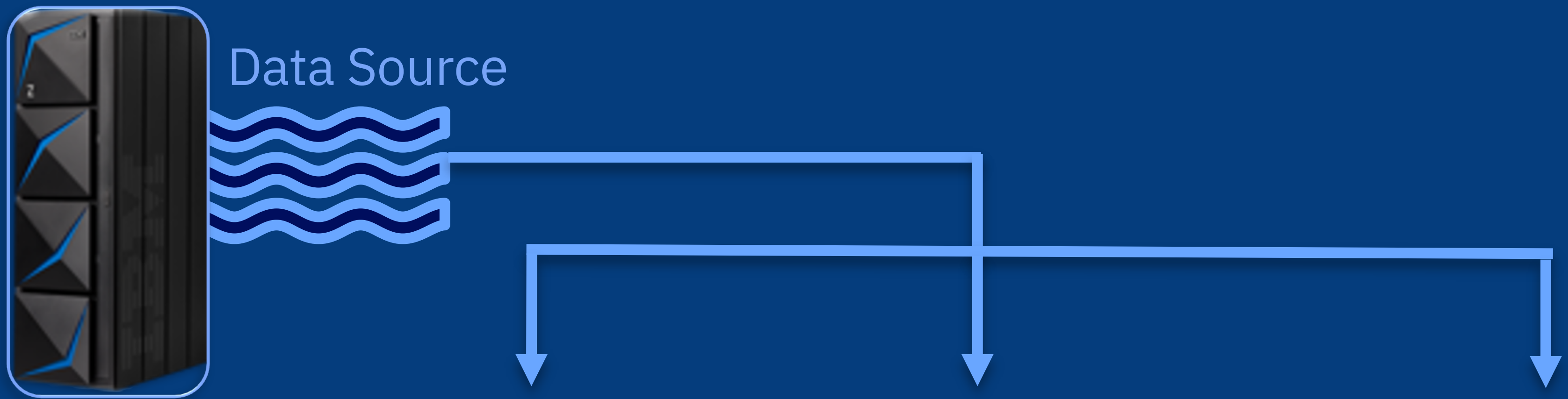


*: Most of the time.

IBM Data Privacy Passports **enforces** and **protects** data


Any distributed DBMS (x86, s390X, Power...)
JDBC able DBMS
IBM Z DBMS
Pervasive Encryption Encryption
z/OS Db2
IBM DVM
VSAM or Sequential
JDBC
IBM Data Privacy passports
Policy
Data Enforcement
Data Protection
Enforce data at the point of consumption
Protect data at the point of exfiltration
JDBC
API
JDBC, SFTP
Data Administrator
Data Owner
Data Consumer
Data Consumer Target DBMS

IBM Data Privacy Passports enforces data



Data Administrator

f_name	l_name	age
XXXXX	XXXXX	XXXXX
XXXXX	XXXXX	XXXXX

ALL fields are masked and displayed

Data Owner

f_name	l_name	age
Alexander	Edwards	20
Lynn	Scott	27

ALL fields are unencrypted and displayed

Data Consumer

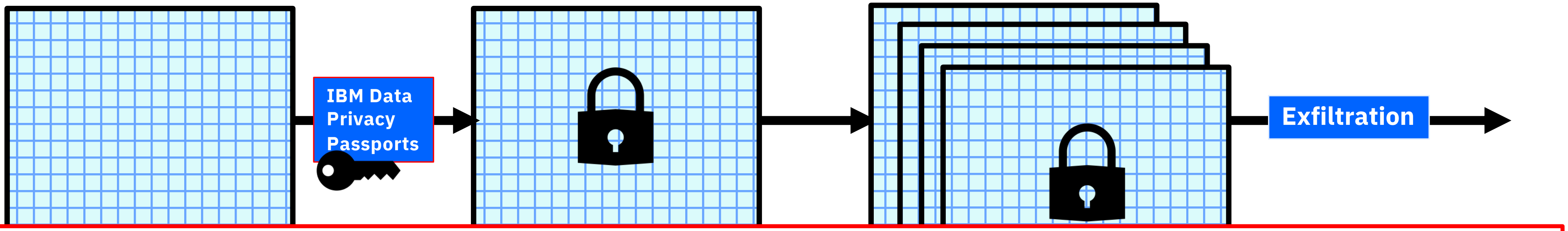
f_name	l_name	age
XXXXX	XXXXX	20
XXXXX	XXXXX	27

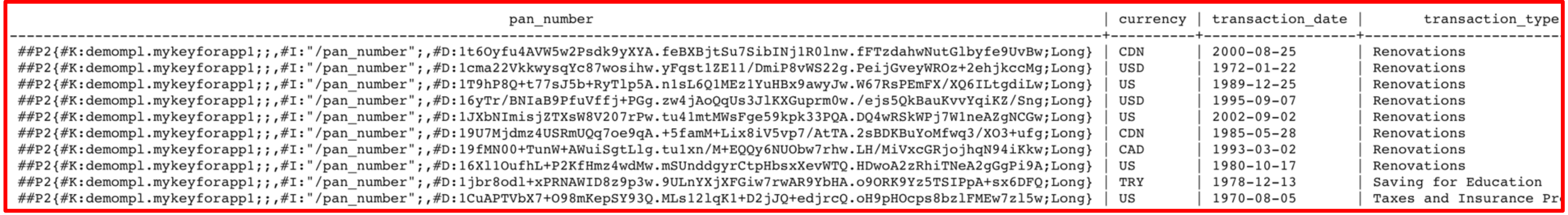
Several fields are masked, some are in the clear and displayed

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

IBM Data Privacy Passports **protects** data, and copies...

- Utilize the basic principle of data centric protection
- Protect critical information as it leaves IBM Z / LinuxONE by policy
- All copies retain protection
- Opening the data requires a return trip to the Passport Controller or to use API



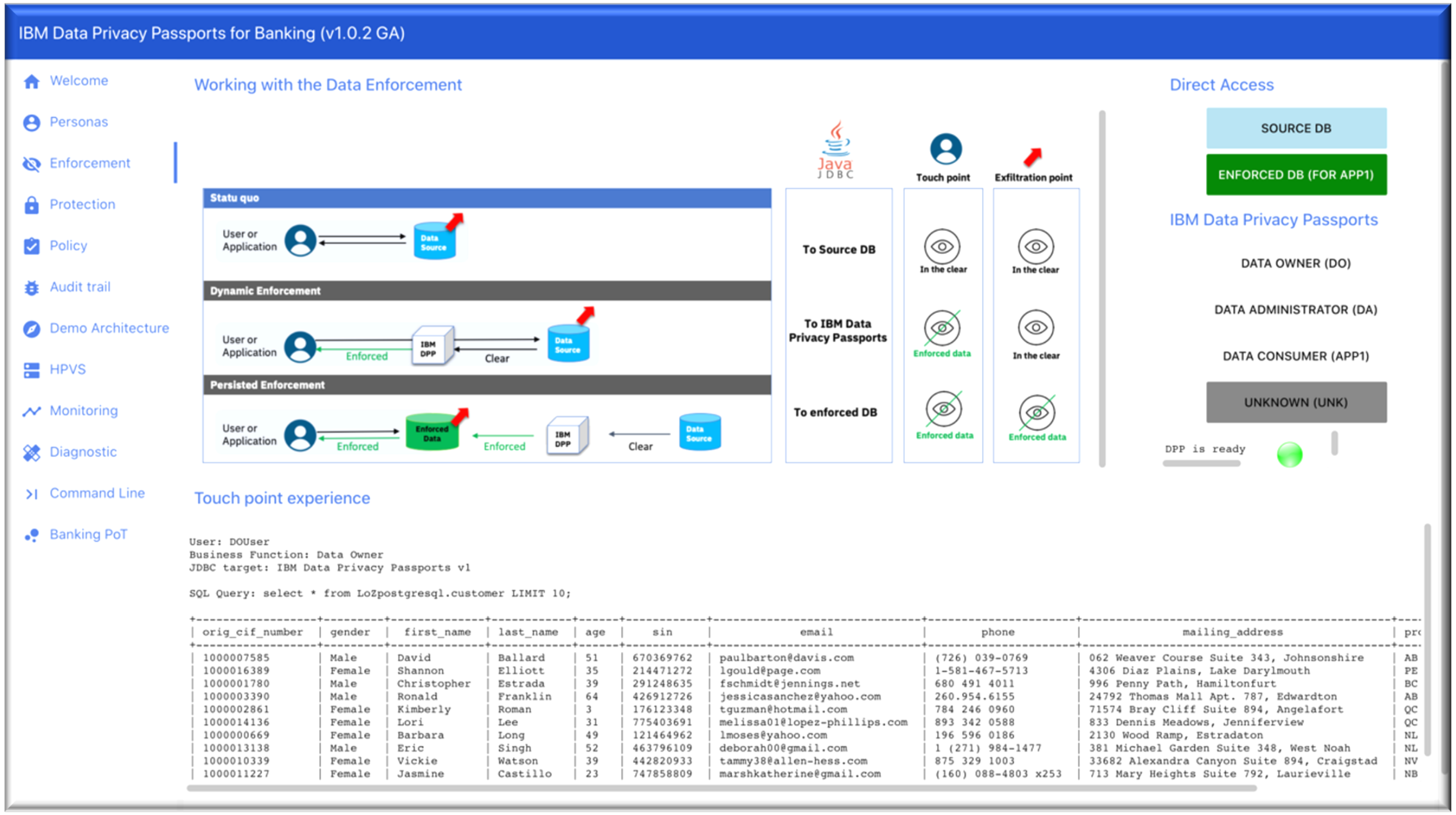


```
                                        pan_number                                                         | currency | transaction_date |     transaction_type
-----------------------------------------------------------------------------------------------------------+----------+------------------+------------------------
 ##P2{#K:demompl.mykeyforappl;;,#I:"/pan_number";,#D:1t6Oyfu4AVW5w2Psdk9yXYA.feBXBjtSu7SibINj1R0lnw.fFTzdahwNutGlbyfe9UvBw;Long} | CDN      | 2000-08-25       | Renovations
 ##P2{#K:demompl.mykeyforappl;;,#I:"/pan_number";,#D:1cma22VkkwysqYc87wosihw.yFqst1ZE11/DmiP8vWS22g.PeijGveyWROz+2ehjkccMg;Long} | USD      | 1972-01-22       | Renovations
 ##P2{#K:demompl.mykeyforappl;;,#I:"/pan_number";,#D:1T9hP8Q+t77sJ5b+RyTlp5A.n1sL6Q1MEz1YuHBx9awyJw.W67RsPEmFX/XQ6ILtgdiLw;Long} | US       | 1989-12-25       | Renovations
 ##P2{#K:demompl.mykeyforappl;;,#I:"/pan_number";,#D:16yTr/BNIaB9PfuVffj+PGg.zw4jAoQqUs3JlKXGuprm0w./ejs5QkBauKvvYqiKZ/Sng;Long} | USD      | 1995-09-07       | Renovations
 ##P2{#K:demompl.mykeyforappl;;,#I:"/pan_number";,#D:1JXbNImisjZTXsW8V207rPw.tu41mtMWsFge59kpk33PQA.DQ4wRSkWPj7W1neAZgNCGw;Long} | US       | 2002-09-02       | Renovations
 ##P2{#K:demompl.mykeyforappl;;,#I:"/pan_number";,#D:19U7Mjdmz4USRmUQq7oe9qA.+5famM+Lix8iV5vp7/AtTA.2sBDKBuYoMfwq3/XO3+ufg;Long} | CDN      | 1985-05-28       | Renovations
 ##P2{#K:demompl.mykeyforappl;;,#I:"/pan_number";,#D:19fMN00+TunW+AWuiSgtLlg.tu1xn/M+EQQy6NUObw7rhw.LH/MiVxcGRjojhqN94iKkw;Long} | CAD      | 1993-03-02       | Renovations
 ##P2{#K:demompl.mykeyforappl;;,#I:"/pan_number";,#D:16Xl1OufhL+P2KfHmz4wdMw.mSUnddgyrCtpHbsxXevWTQ.HDwoA2zRhiTNeA2gGgPi9A;Long} | US       | 1980-10-17       | Renovations
 ##P2{#K:demompl.mykeyforappl;;,#I:"/pan_number";,#D:1jbr8odl+xPRNAWID8z9p3w.9ULnYXjXFGiw7rwAR9YbHA.o9ORK9Yz5TSIPpA+sx6DFQ;Long} | TRY      | 1978-12-13       | Saving for Education
 ##P2{#K:demompl.mykeyforappl;;,#I:"/pan_number";,#D:1CuAPTVbX7+O98mKepSY93Q.MLs12lqK1+D2jJQ+edjrcQ.oH9pHOcps8bzlFMEw7zl5w;Long} | US       | 1970-08-05       | Taxes and Insurance Pr
```

Agenda

- Rapid introduction of IBM Data Privacy Passports
- **IBM Data Privacy Passports in action**

It is time for a Demo !



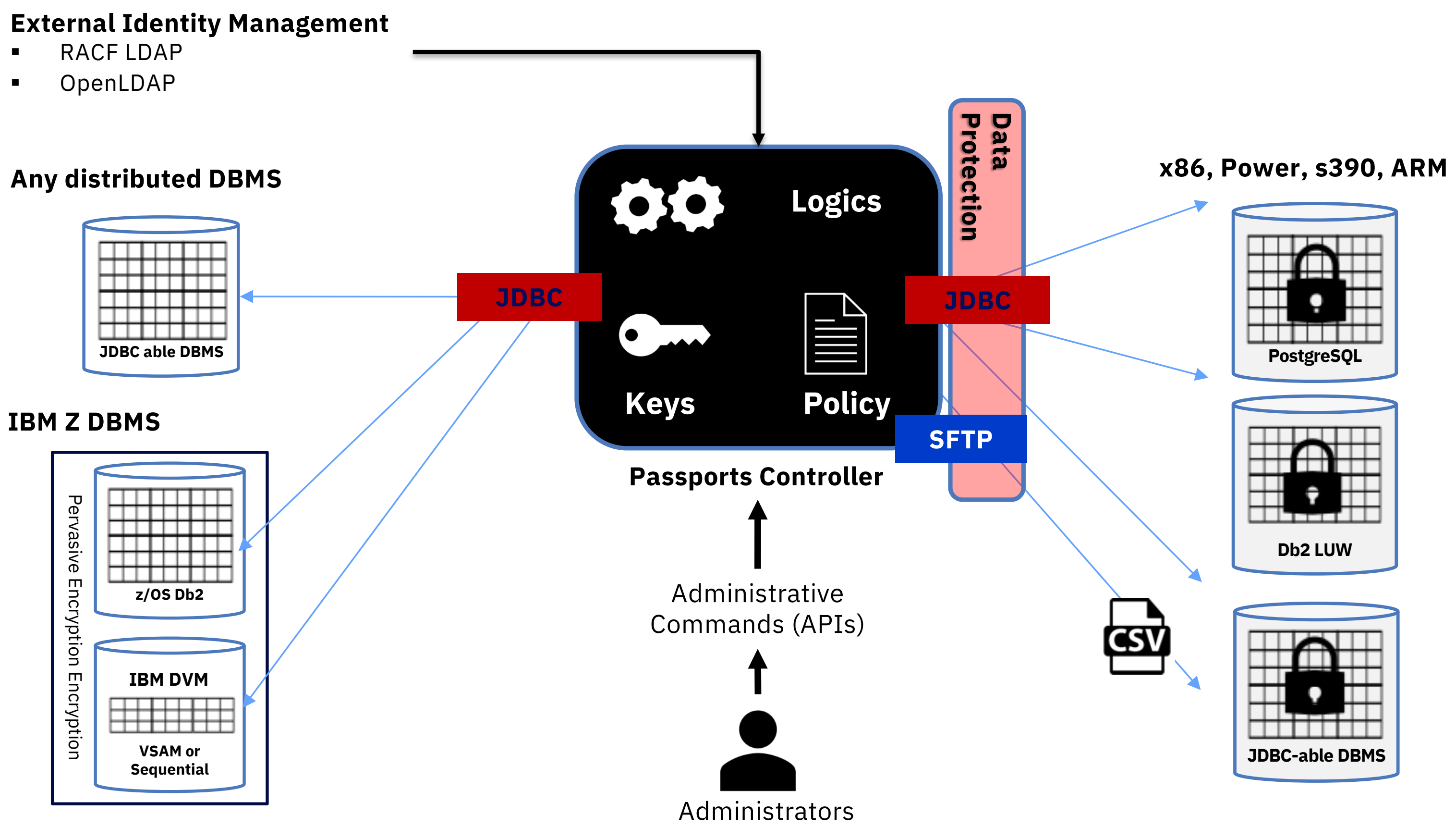
Touch point experience

```
User: DOUser
Business Function: Data Owner
JDBC target: IBM Data Privacy Passports v1

SQL Query: select * from LoZpostgresql.customer LIMIT 10;

+-----------------+--------+--------------+------------+-----+------------+---------------------------+----------------------+-----------------------------------------------------+----
| orig_cif_number | gender |  first_name  | last_name  | age |    sin     |           email           |        phone         |                   mailing_address                   | pr
+-----------------+--------+--------------+------------+-----+------------+---------------------------+----------------------+-----------------------------------------------------+----
| 1000007585      | Male   | David        | Ballard    | 51  | 670369762  | paulbarton@davis.com      | (726) 039-0769       | 062 Weaver Course Suite 343, Johnsonshire           | AB
| 1000016389      | Female | Shannon      | Elliott    | 35  | 214471272  | lgould@page.com           | 1-581-467-5713       | 4306 Diaz Plains, Lake Darylmouth                   | PE
| 1000001780      | Male   | Christopher  | Estrada    | 39  | 291248635  | fschmidt@jennings.net     | 680 491 4011         | 996 Penny Path, Hamiltonfurt                        | BC
| 1000003390      | Male   | Ronald       | Franklin   | 64  | 426912726  | jessicasanchez@yahoo.com  | 260.954.6155         | 24792 Thomas Mall Apt. 787, Edwardton               | AB
| 1000002861      | Female | Kimberly     | Roman      | 3   | 176123348  | tguzman@hotmail.com       | 784 246 0960         | 71574 Bray Cliff Suite 894, Angelafort              | QC
| 1000014136      | Female | Lori         | Lee        | 31  | 775403691  | melissa01@lopez-phillips.com | 893 342 0588      | 833 Dennis Meadows, Jenniferview                    | QC
| 1000000669      | Female | Barbara      | Long       | 49  | 121464962  | lmoses@yahoo.com          | 196 596 0186         | 2130 Wood Ramp, Estradaton                          | NL
| 1000013138      | Male   | Eric         | Singh      | 52  | 463796109  | deborah00@gmail.com       | 1 (271) 984-1477     | 381 Michael Garden Suite 348, West Noah             | NL
| 1000010339      | Female | Vickie       | Watson     | 39  | 442820933  | tammy38@allen-hess.com    | 875 329 1003         | 33682 Alexandra Canyon Suite 894, Craigstad         | NV
| 1000011227      | Female | Jasmine      | Castillo   | 23  | 747858809  | marshkatherine@gmail.com  | (160) 088-4803 x253  | 713 Mary Heights Suite 792, Laurieville             | NB
```

Demo Agenda

- Overview
- Personas and Privacy
- Data Enforcement
- Data Protection
- Policy content, elements
- …

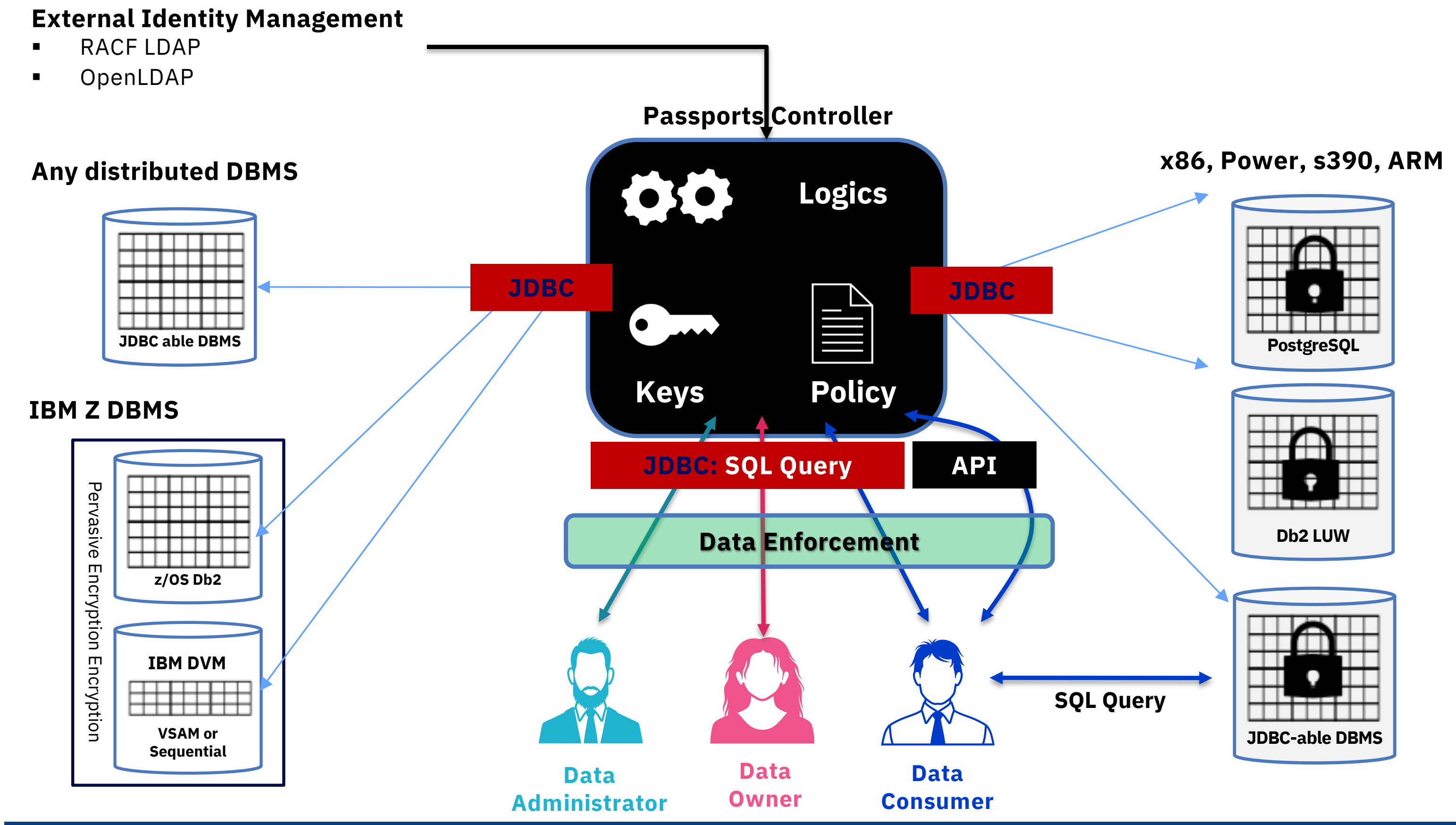
Protect Data In the Enterprise (1/2)



To keep in mind

- Passport Controller deployed in an SSC LPAR. So, the **Policy** resides in the safer IBM Z / LinuxONE environment.
- Data is **protected** at the point of extraction and is **enforced** at the point of consumption.
- Move data from/to as **Trusted Data Objects** requires JDBC connections or .csv SFTP transfer.
- JDBC is required to connect DBMS and to SQL Query IBM Data Privacy Passports.
- **Create a single protected table to provide multiple views of data**

Protect Data In the Enterprise (2/2)



To keep in mind

- Enforce data on distributed platform using Passport Controller on IBM Z / LinuxONEat the time of consumption
- Identity can be managed on IBM Z and LinuxONE via RACF LDAP or OpenLDAP.
- Policy for enforcement can be changed dynamically to revoke to entitle users to data
- APIs to enforce data, and to protect data on the flight.

- **Connection to Passport Controller through industry standard Apache Hive drivers.**

Hardware/Software pre-requisites

Hardware:

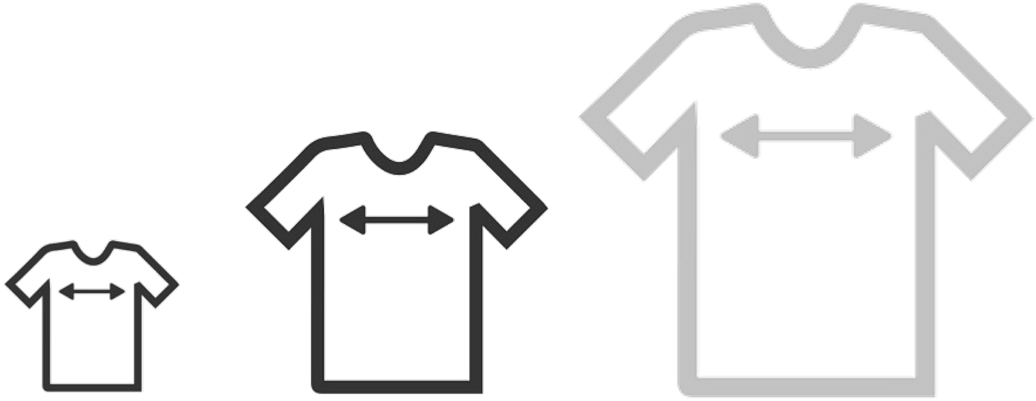
- z15 or LinuxONE III
- FC104
- Networking
- Dedicated IFLs
- Dedicated Memory

Software:

- ***Hyper Protect Virtual Server*** PID (This is the secure host of IBM Data Privacy Passports).

Other:

- Linux Machine (x86 or s390x) for HPVS and IBM Data Privacy Passport deployment purpose. It requires support of Python 3.8.



	GCP or IFL (SMT-2)	Memory	Disk Storage
Small	4	128GB	128GB
Medium	8	256GB	256GB

Thank you

guillaume_hoareau@fr.ibm.com

Certified IT Architect, IBM Z Security
IBM Systems Lab Services, Europe