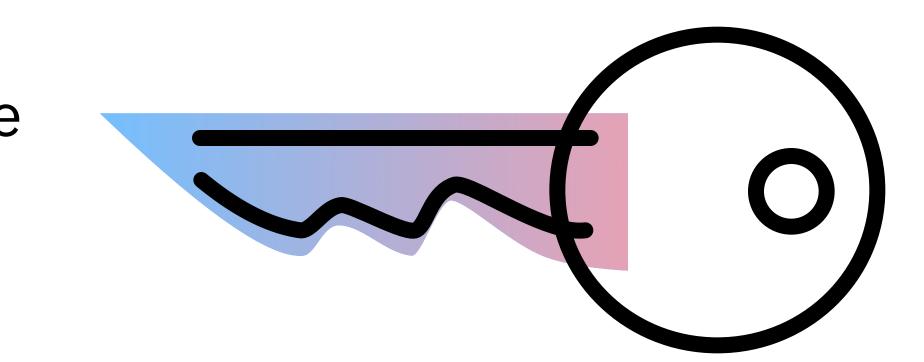
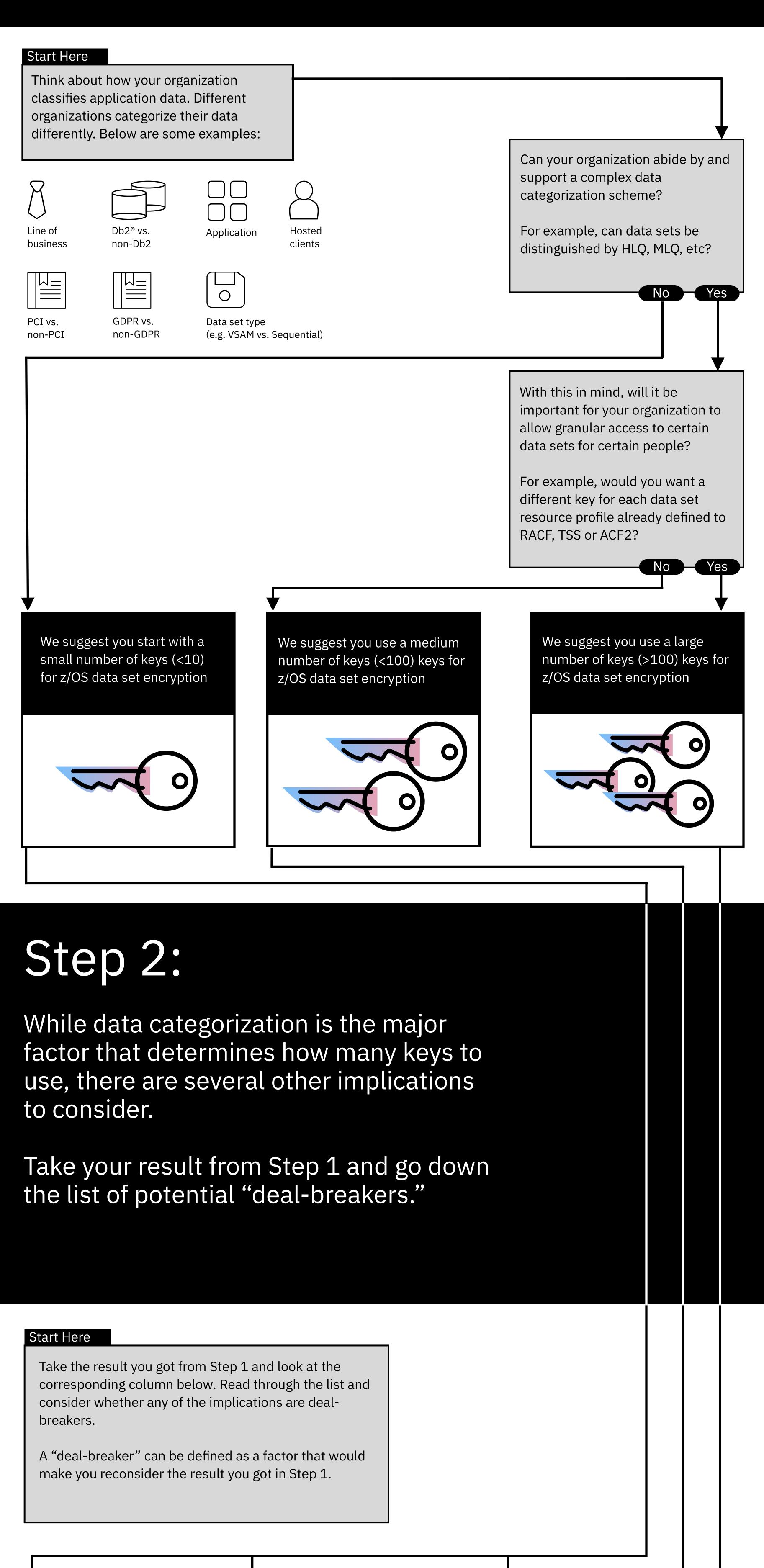
How many keys should you use for z/OS® data set encryption? Let's find out!

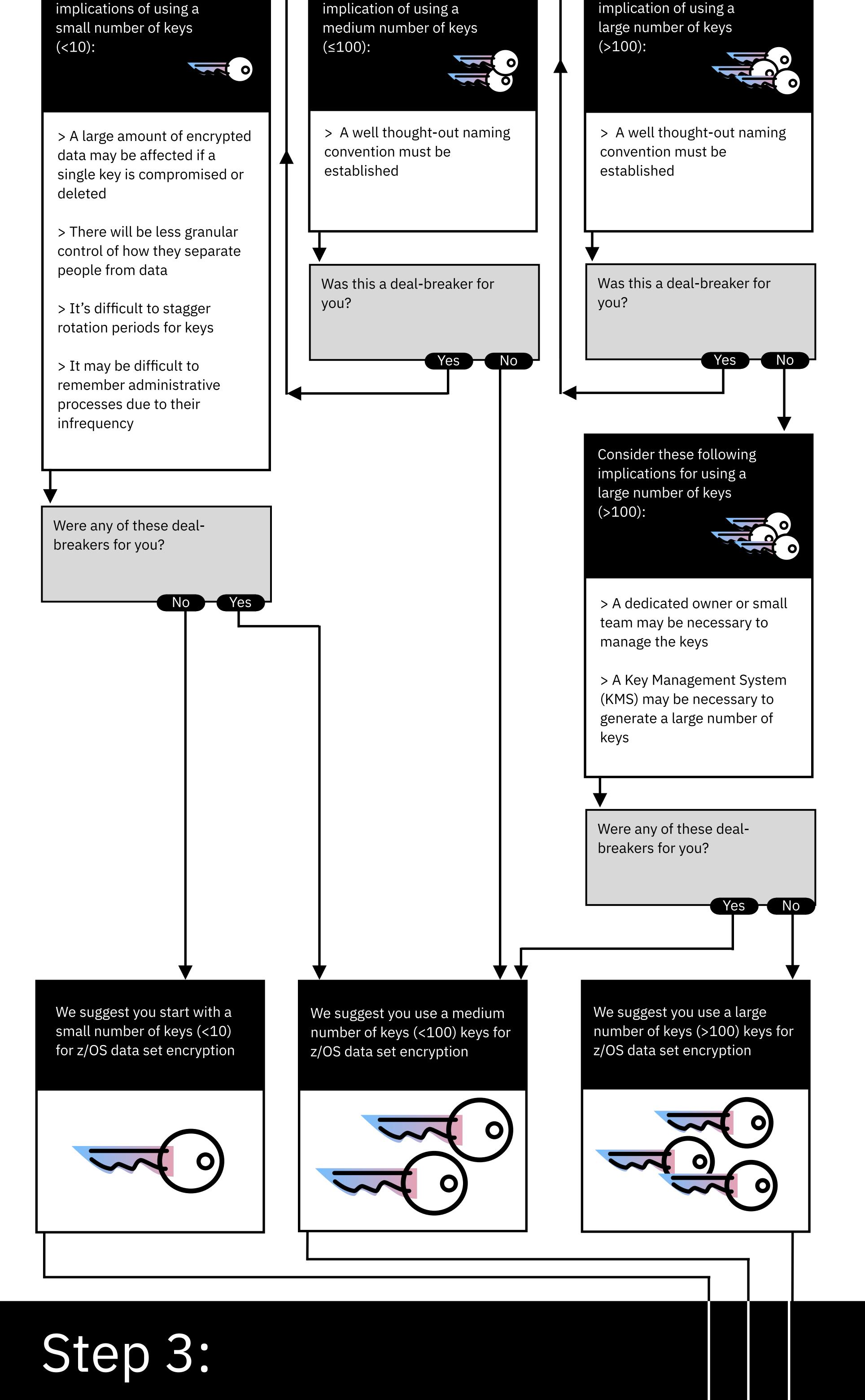


Step 1:

Start by asking yourself the following: How are your data sets categorized and organized today?

Follow the steps below to understand how many keys you should use:





Consider the following

Consider the following

Consider the following

your environment.

Do you want any of the following features? Do you plan to do periodic key rotation in a such a way > Easy viewing of keys that the number of keys would grow beyond 10? > Key store backup and easy recovery of a single key OR > Key versioning from a centralized solution If you plan to distribute keys > Automatic key propagation to a Disaster Recovery to other Integrated system Cryptographic Service Facility (ICSF) key stores > Strong dual-control of key management operations

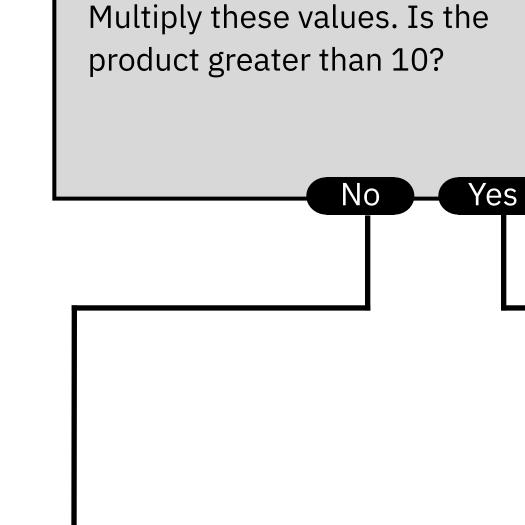
In some cases, it may be necessary to

Management Foundation (EKMF) into

Is this the case for you? Let's find out:

system such as the Enterprise Key

integrate a centralized key management



Result:

EKMF is optional

Based on your choices,

EKMF may not be

necessary.

with different master keys,

a) How many LPARs need to

b) How many keys need to

be sent from one LPAR to

another on average?

consider the following:

receive the key?

distribution of a key and its versions? Yes Do you need any of the following features?

Are you able to manually facilitate the

applications

> Bulk key creation

EKMF Web is recommended

Based on your choices, we

Contact ibmsls@us.ibm.com

recommend EKMF Web.

for more information.

Result:

EKMF Workstation is recommended

> Management of keys for other purposes and

Result:

No

No

Based on your choices, we

recommend the EKMF

Workstation. Contact

more information.

ibmsls@us.ibm.com for

For more information on z/OS Data Set Encryption or pervasive encryption on Z®, visit:

https://www.ibm.com/support/z-content-solutions/pervasive-encryption/