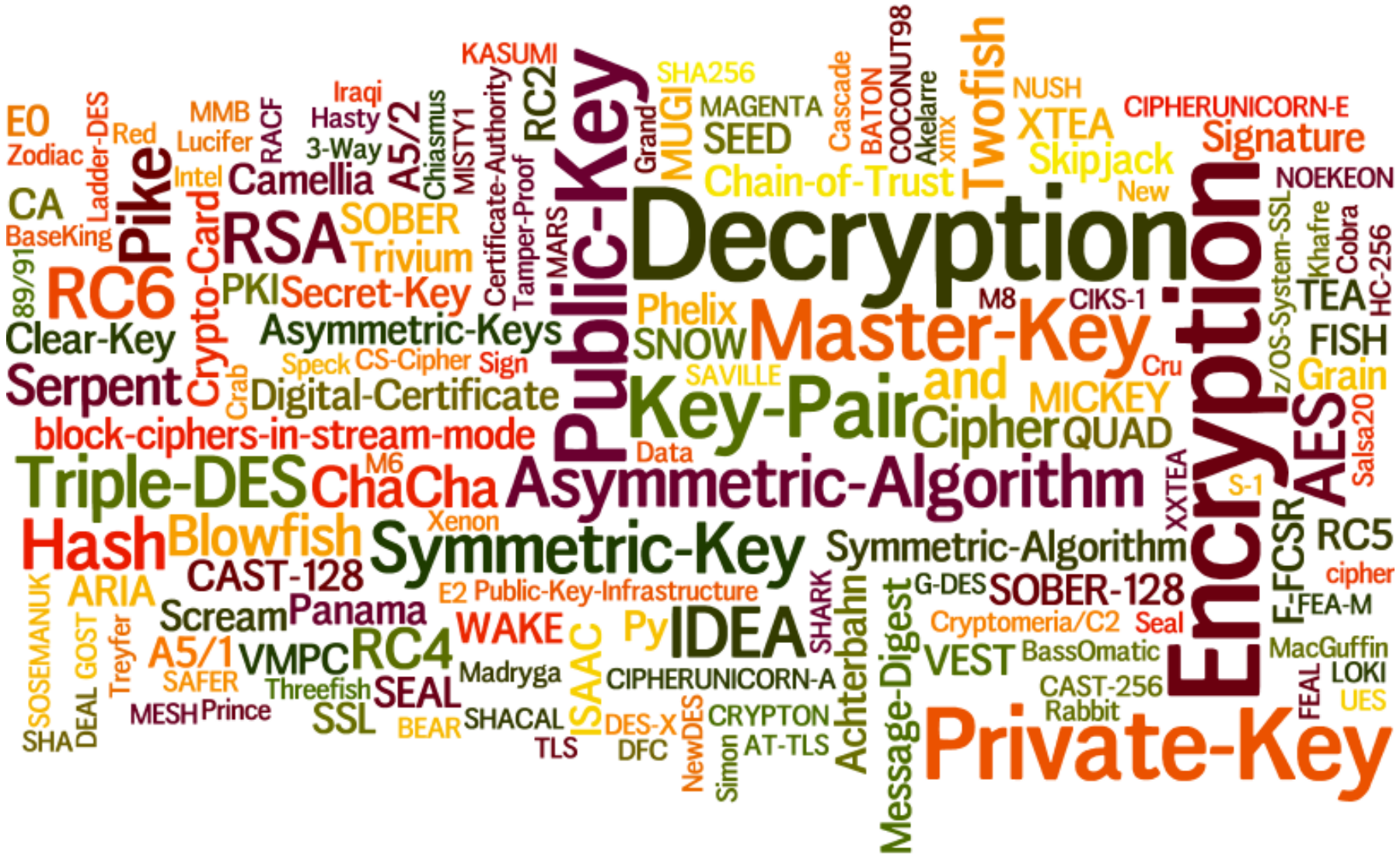
Cryptography on IBM Z and z/OS

GSE zExpertenforum April 2018

Peter Hunkeler
UBS Business Solutions AG

Cryptography – Cryptography? – Cryptography!



Encryption on IBM Z and IBM z/OS

- IBM initiative to encrypt data on z/OS.
- First steps:
  - Encrypt data sets on z/OS
  - Encrypt Coupling Facility structures
- Use specialised hardware
  - Crypto Express cards
- Prevent enrcyption keys to appear in clear in memory or elsewhere
  - ICSF and Crypto Express
  - Master Key kept inside tamper detecting hardware
  - ICSF maintains keys in keys stores. Keys are encrypted with Master Key

Compression/Encryption on Device versus on z/OS

- Modern Disk and Tape systems offer to encrypt data when written
- Modern Disk and Tape systems compress data to save space.
  - Compression is done before encryption

- z/OS Pervasive Encryption encrypts data before if is sent to the device.
  - Comperssion on decive will no longer save much space
  - Compress data on z/OS before encrypting and sending to device

Clear Key, Secure Key and Protected Key

- **Clear Key** – Clear Key refers to key material that is in the clear, meaning the clear key value appears within application storage and within the keystore.
- **Secure Key** - Provides high security because the key material is encrypted by a Master Key. Neither the Master Key nor any key material does ever appear in clear outside of the special tamper proof hardware (Crypto Express cards).
- **Protected Key** - Hperformance and high security solution by taking advantage of the high speed CPACF while utilizing symmetric keys protected by the cryptographic coprocessor Master Key.
  - A *Wrapper Key* is generated by the IBM Z hardware upon LPAR activation. This key is kept in HAS (hardware storage area)
  - User keys are decrypted, then encrypted using the *Wrapper Key* which is then used inside the CPACF.

Master Key Renewal

- The Master Keys are only ever used to encrypt and decrypt application *keys*.
  - No application *data* is ever encrypted with Master Keys.
- Renewing Master Keys means replacing the old Master Keys with new Master Keys.
  - Any application key protected by a Master Key must be decrypted using the old Master Key, then encrypted by the new Master Key.
  - No application *data* has to be touched.