3.11 Secure Service Container

Client applications are subject to a number of security risks in a production environment. These risks might include external risks (cyber hacker attacks) or internal risks (malicious software, system administrators using their privileged rights for unauthorized access and many others).

Secure Service Container (SSC) is an integrated IBM Z appliance and is designed to host most sensitive client workloads and applications, acting as a highly protected and secured digital vault, enforcing security by encrypting the whole stack: memory, network and data (both in-flight and at-rest). Applications running inside SSC are isolated and protected from outsider and insider threats.

SSC combines hardware, software, and middleware and is unique to IBM Z platform. Though it is called a container, it should not be confused with purely software open source containers (such as Kubernetes or Docker).

SSC is a part of the Pervasive Encryption concept that was introduced with IBM z14, which is aimed at delivering best IBM Security hardware and software enhancements, services, and practices for 360 degree infrastructure protection.

LPAR is defined as SSC by using the Hardware Management Console (HMC).

The SSC solution includes the following key advantages:

- Existing applications require zero changes to use SSC; software developers do not need to write any SSC specific programming code.
- End-to-end encryption, both of in-flight and at-rest data:
  - Automatic Network Encryption (TLS, IPSEC): Data-in-flight.
  - Automatic File System Encryption (LUKS): Data-at-rest.
  - Linux Unified Key Setup (LUKS) is the standard way in Linux to provide disk encryption. SSC encrypts all data with a key that is stored within the appliance.
  - Protected memory: Up to 16 TB can be defined per SSC LPAR.
- Encrypted Diagnostic Data

  All diagnostic information (debug dump data, logs) are encrypted and do not contain any user or application data.
- No operating system access:

  After the SSC appliance is built, Secure Shell (SSH) and command line-interface (CLI) are disabled, which ensures that even system administrators do not have access to the contents of SSC and do not know what application is running there.
- Applications that run inside SSC are being accessed externally by REST APIs only, in a transparent to user way.
- Tamper-proof SSC Secure Boot:
  - SSC- eligible applications are being booted into SSC by using verified booting sequence, where only trusted and digitally signed and verified by IBM software code is uploaded into the SSC.
  - Vertical workload isolation, certified by EAL5+ Common Criteria Standard, which is the highest level that ensures workload separation and isolation.
  - Horizontal workload isolation: Separation from the rest of the host environment.