

Measuring Crypto Activities Performance in z/OS – Part 1

Fabio Massimo Ottaviani

January 2019

1 Introduction

Internet and online services are currently used to transfer data and process the transactions completed by billions of people. This is the reason why cryptography, which lies at the core of digital security, is becoming more and more important for every company. The primary functions of cryptography are:

- Identification and authentication, to identify users to the system and provide proof that they are who they claim to be
- Access control, to determine which users can access which resources
- Data confidentiality, to ensure that no one can read the data except the intended receiver
- Data integrity, to assure the receiver that the received data have not been altered in any way from the original
- Security management, to administer and control a security policy, including key management
- Nonrepudiation, to prove that the sender really sent this message and the receiver received it

As you can imagine cryptographic services need to use hardware resources (mostly CPU) and have an impact on application performance.

In this paper after a short overview of software and hardware cryptographic facilities available in z/OS, we will discuss the most important metrics provided in SMF records to evaluate CPU usage and performance of cryptographic activities.