



QuinStreet ●●● 10400 Linn Station Road, Suite 100 ●●● Louisville, KY 40223

Cryptographic Key Management Issues & Challenges in Cloud Services

Encryption and access control are the two primary means for ensuring data confidentiality in any IT environment. In situations where encryption is used as a data confidentiality assurance measure, the management of cryptographic keys is a critical and challenging security management function, especially in large enterprise data centers, due to sheer volume and data distribution (in different physical and logical storage media), and the consequent number of cryptographic keys. This function becomes more complex in the case of a cloud environment, where the physical and logical control of resources (both computing and networking) is split between cloud actors (e.g., consumers, providers, and brokers).

The objectives of this document are to identify:

- (a) The cryptographic key management issues that arise due to the distributed nature of IT resources, as well the distributed nature of their control, the latter split among multiple cloud actors. Furthermore, the pattern of distribution varies with the type of service offering - infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS).
- (b) The special challenges involved in deploying cryptographic key management functions that meet the security requirements of the cloud consumers, depending upon the nature of the service and the type of data generated/processed/stored by the service features.

The attached zip file includes:

- Intro Page.pdf
- Terms and Conditions.pdf
- CryptographicKeyMgmt.pdf