# Enterprise Key Management Challenges and Framework

Chii-Ren Tsai

Citigroup O&T Risk Management
12401 Prosperity Drive
Silver Spring, MD 20904
chiiren.tsai@citi.com

**Abstract**

Enterprises have deployed numerous home-grown and/or commercial-off-the-shelf cryptographic solutions. A major challenge is many solutions were deployed without any specific KM tool to manage keys throughout their life cycles. Consequently, manual processes must be created to bridge the gap and mitigate the risk to certain extent. A small number of solutions are equipped with a KM tool to manage keys used by applications or unattended processes. However, they tend to be proprietary and are not interoperable with other solutions.

It is foreseeable that some KM tools will emerge to manage keys in heterogeneous platforms or systems. To allow such tools to support both legacy and newly developed KM systems, it may be necessary to ensure they are architected and developed based on an industry-wide KM implementation framework that may contain reference architectures, guidelines, common APIs and protocols. To delineate such a framework for enterprise key management, we would suggest the following for consideration:

- Create separate KM domains by grouping keys with similar life cycle and KM functions in the same domain. Such breakdown is meant to avoid conflicting requirements and reduce the complexity of tool development.

- Impose the creation of a secure key store in each server to become the central repository of keys for various applications. APIs and access control mechanisms can be created. The key store could be a software vault or HSM.

- Keys should be created and stored as “objects” in key stores, such that attributes, access control and policy can be specified and enforced.

- Leverage or incorporate industry KM efforts, such as OASIS KMIP, KM functions and APIs in various crypoAPIs, PKCS#11 or HSMs, into the framework.