1. **What is being announced?**

   OASIS along with Brocade, EMC, HP, IBM, LSI, Netapp, Seagate and Thales are announcing the creation of a Key Management Interoperability Protocol (KMIP) Technical Committee to complete the group's work on an open standards track.

2. **What problem does it solve?**

   The problem addressed by KMIP is primarily that of standardizing communication between encryption systems that need to consume keys and the key management systems that create and manage those keys. Being able to encrypt and retain access to data requires that encryption keys be generated and stored. To date, organizations deploying encryption have not been able to take advantage of interoperability across encryption and the key management systems.

3. By defining a low-level protocol that can be used to request and deliver keys between any key manager and any encryption system, KMIP enables the industry to have any encryption system communicate with any key management system. Through this interoperability, enterprise will be able to deploy a single enterprise key management infrastructure to mange keys for all encryption systems in the enterprise that require symmetric keys, asymmetric keys pairs, certificates and other security objects.

4. **What does the OASIS KMIP Technical Committee do?**

   The OASIS KMIP TC focuses on the development of a standard key management interoperability protocol. "KMIP" stands for "Key management Interoperability Protocol".

5. **What is the need for such a standard?**

   Today's enterprises operate in an increasingly complex, multi-vendor environment. At the same time, they are facing budget challenges in the current economic situation and must be mindful of potentially expensive integration projects. Organizations have a desire to deploy encryption across the enterprise; and are unclear on how to do that. They often deploy separate encryption for different business uses –laptops, storage, databases and applications, resulting in:

   - Cumbersome –often manual –efforts necessary to generate, distribute, vault, expire, and rotate encryption keys.
   - Increased costs for IT, challenges meeting audit and compliance requirements, and lost data.

   In general, enterprises have a lack of confidence that, once encrypted, IT managers will be able to actually recover the encrypted data when they'll need to. IDC found the #1 and #2 barriers to deploying encryption were "reliability" and "data recoverability" or simply stated: "the biggest barrier to the widespread use of storage encryption is the fear that encrypted data will be lost."

6. **Who will benefit from KMIP and how?**

   Every developer, user, or maintainer of applications that require key management will benefit.

7. **How does this work compare with related standards efforts?**

   No other key management efforts encompass the scope of KMIP. The OASIS KMIP TC is aware of several related efforts:

   - OASIS EKMI TC. We see KMIP TC as addressing a broader scope than the primarily symmetric key focused EKMI, providing a more comprehensive protocol in which SKSML can potentially participate.

- IEEE P1619.3. We see KMIP TC as addressing a broader scope than the primarily storage-related P1619.3.
- TCG Infrastructure Working Group. We see KMIP TC as addressing a broader scope than the primarily TPM-related TCG IWG.
- IETF Keyprov. We see KMIP TC as addressing a broader scope than the primarily mobile-related-related IETF Keyprov.

8. What are the current activities of the OASIS KMIP TC?

There are pointers to our current working drafts on the OASIS KMIP TC public home page.

9. Where are the archives for the OASIS KMIP TC mailing lists?

The archives are located at the OASIS KMIP Home Page These are publicly viewable.

10. Who should be involved in the OASIS KMIP TC?

Architects, designers and implementers of providers and consumers of enterprise key management services.

11. When does the OASIS KMIP TC meet?

General body proposed meetings are to be held by teleconference every week.

12. Where do I use this technology?

Anywhere you need key management services for both management servers and devices or applications that perform encryption.

13. Where should I expect vendors to be using this technology?

The standard will likely first be implemented in products such as key management servers and controlling devices.