d) A clear English-language summary of the specification;

The Key Management Interoperability Protocol (KMIP) establishes a single, comprehensive protocol for communication between enterprise key management servers and cryptographic clients. By defining a protocol that can be used by any cryptographic client, from the smallest automated electric meters to the most complex disk-arrays, KMIP enables key management servers to speak a single protocol to all cryptographic clients supporting the protocol. Through vendor support of KMIP, an enterprise will be able to consolidate key management in a single key management system, reducing operational and infrastructure costs while strengthening operational controls and governance of security policy.

KMIP includes three primary elements:

* Objects. These are the symmetric keys, asymmetric keys, digital certificates and so on upon which operations are performed.
* Operations. These are the actions taken with respect to the objects, such as getting an object from a key management system, modifying attributes of an object and so on.
* Attributes. These are the properties of the object, such as the kind of object it is, the unique identifier for the object, and so on.

At its most basic level, KMIP consists of placing objects, operations and/or attributes either into a request from a cryptographic client to a key management server or into a response from a key management server to a cryptographic client. The protocol also supports other elements, such as the use of templates that can simplify the specification of attributes in a request or response.

(e) A statement regarding the relationship of this specification to similar work of other OASIS TCs or other standards developing organizations;

As a transport-level protocol, KMIP is complementary to other key management efforts, , expressed in XML, including OASIS EKMI. KMIP leverages other standards whenever possible. For example, it uses the key life-cycle specified in NIST special publication 800-57 to define attributes related to key states. It uses network security mechanisms such as TLS to establish authenticated communication between the key management system and the cryptographic client. It relies on existing standards for encryption algorithms, key derivation and many other aspects of a cryptographic solution, focusing on the unique and critical problem of interoperable messages between key management systems and cryptographic clients.