ReKey and ReKeyKeyPair Proposal

The ballot created based on the motion from Bruce Rich (IBM) and John Leiseboer (Quintessence Labs) requests the KMIP technical committee accept a proposal to change the specification of two existing operations.

Cryptsoft believes that TC members should vote No to this proposal for the following reasons:

1. Altering the operations to make them no longer analogous to Create and CreateKeyPair is a fundamental change in the semantics of these operations. ReKey and ReKeyKeyPair are effectively a create operation using an existing managed object as a "template" with a couple of additional rules to handle adjusting life-cycle dates, moving the (unique) Name from the retired object to the new object; and maintaining links between the objects.
2. The changes specify that a conforming server is either allowed to accept and process attributes or to return an error (*server SHOULD return an error*) – both approaches are permitted. A client has no way to determine which behaviour a server will accept.
3. The specification of SHOULD rather than SHALL was done to make the change seem less radical as the existing implemented behaviour would remain permitted – however this simply specifies non-interoperability – allowing two incompatible options where a client has no way to determine which will be accepted without trying one and then the other.
4. Fundamentally changing the definition of operations in a minor release of a specification without a clearly demonstrated (real) interoperability issue between multiple vendors is unwarranted.
5. Multiple vendors have already implemented and deployed ReKey and ReKeyKeyPair support and "complexity of implementation" as an argument to change the specification is at best untimely.

Specifics additional issues in the proposal:

6. Listing Fresh in table 131 and 135 is inconsistent – it is not listed in the other "create" operations. It should either be listed in DeriveKey and ReCertify or not be added to ReKey and ReKeyKeyPair. The definition of Fresh in 3.34 is clear. Lease Time isn't noted so why is Fresh?
7. The change to Usage Limits to state "In either case, the Count value is set to the Total value in the existing key" is simply incorrect handling of Usage Limits. The Count value must be set to the Total value for the new object – **not** from the existing (previous) object when the Total value has been replaced by the caller providing a new value. See 3.21 *"When the attribute is initially set (usually during object creation or registration), the Usage Limits Count is set to the Usage Limits Total value allowed for the useful life of the object, and are decremented when the object is used.*"
8. KMIP is a protocol – not an API – so statements like "Although the API" should not be added into the protocol specification.
9. Introducing a new term "active key lifecycle" should not be done within the specification of an operation. If we want to use that sort of term it belongs in the main definitions.