

TPM \rightarrow KeyStorage (parameters)

TPM \rightarrow Alice: PrivateKey. Rec a

Read: Alice \rightarrow TPM : Read. PCR \rightarrow TPM : value. TPM \rightarrow PCR : value. TPM \rightarrow Alice : value

Quote: Alice \rightarrow TPM : Quote. PCR \rightarrow TPM : vale. TPM \rightarrow PCR : value. TPM \rightarrow Alice : CertPCR

CreateWrapKey: Alice \rightarrow TPM : CreateWrapKey. PCR \rightarrow TPM : value. TPM \rightarrow PCR : value.

KeyTable \rightarrow TPM : KeyLoaded. ?(new key)?. TPM \rightarrow Alice : data?

LoadKey2: Alice \rightarrow TPM : LoadKey2. PCR \rightarrow TPM : value. TPM \rightarrow PCR : value. KeyTable \rightarrow TPM : KeyLoaded.

TPM \rightarrow KeyTable : LeyLoaded

CertifyKey: Alice \rightarrow TPM : data. KeyTable \rightarrow TPM : KeyLoaded. TPM \rightarrow Alice : Cert

Unbind: Alice \rightarrow TPM : unbind. PCR \rightarrow TPM : value. TPM \rightarrow PCR : value. KeyTable \rightarrow TPM : KeyLoaded.

TPM \rightarrow Alice : adec

Seal: Alice \rightarrow TPM : data. PCR \rightarrow TPM : value. TPm \rightarrow PCR : value. KeyTable \rightarrow TPM : KeyLoaded. TPM \rightarrow Alice : data

Unseal: Alice \rightarrow TPM : unseal. PCR \rightarrow TPM : value. TPM \rightarrow PCR : value. KeyTable \rightarrow TPM : KeyLoaded.

TPM \rightarrow Alice : KeyLoaded.

Extend: Alice \rightarrow TPM : extend. PCR \rightarrow TPM : value. TPM \rightarrow PCR : hpcr.