



Option 1a: The MK or a segment of the MK is used as DPK.

Option 1b: The DPK is derived from the MK using an **approved** key derivation function.

Option 2a: The MK is used to recover the DPK through an **approved** authenticated encryption or an **approved** key protection/recovery method.

Option 2b: The key to recover the DPK through an **approved** authenticated encryption or an **approved** key protection/recovery method is derived from the MK using an **approved** key derivation function.

§

LEGAL

(PSEUDO|
ANONYM)ISED?