Revised text in Section 8.3 of X9.82, Part 3 (last para.):

When DRBG mechanism functions are distributed, a secure channel **shall** be used to protect the internal state or parts of the internal state that are transferred between the distributed DRBG mechanism sub-boundaries. The security provided by the secure channel **shall** be consistent with the security required by the consuming application (see ASC X9 Registry).

Definition for X9.82:
Secure channel
A path for transferring data between two entities or components that ensures confidentiality, integrity and replay protection, as well as mutual authentication between the entities or components. The secure channel may be provided using cryptographic, physical or procedural methods, or a combination thereof.

The above definition was adapted from a definition for a trusted channel from Draft 140-3:
Trusted Channel: A mechanism through which a cryptographic module provides a trusted, safe and discrete communication pathway for SSPs and other critical information between itself and its intended communications endpoint. A trusted channel exhibits a verification component that the operator or module may use to confirm that the trusted channel exists. A trusted channel protects against eavesdropping as well as physical or logical tampering by unwanted operators/entities, processes or other devices, both within the module and along its communication link with the intended endpoint (e.g., will not allow man-in-the-middle or replay types of attacks). A trusted channel may be realized in one or more of the following ways:

*	A communication pathway between the cryptographic module and endpoint that is entirely local, directly attached to the cryptographic module and has no intervening systems.
*	A mechanism that cryptographically protects SSPs during entry and output and does not allow misuse of any transitory SSPs.