

Proposed Key States for P1619.3 Architecture

The following diagram depicts modifications to the NIST key state transition diagram found in Special Publication 800-57 and how each state maps to it. Specific information for the NIST key state transition diagram can be found in SP800-57 part 1.

Key States

A recommended model for key states contains the following with recommended state values:

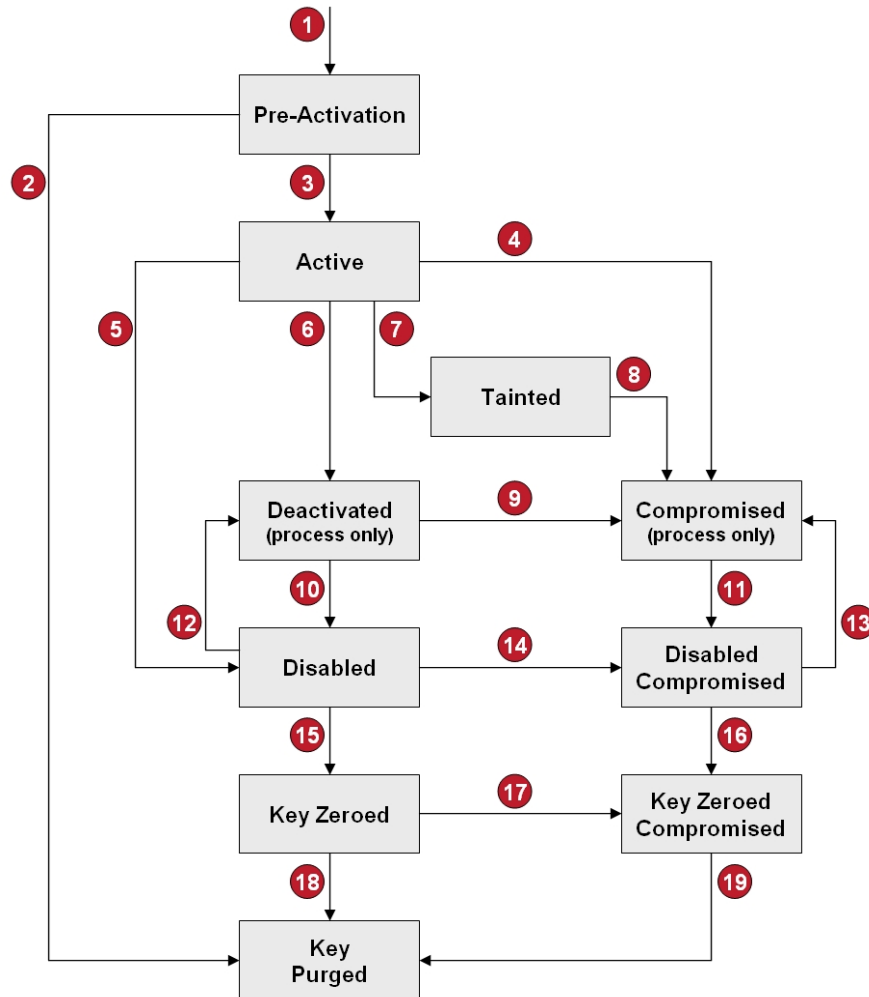
- **Pre-activation** – state 0 – Keys that are generated but not returned to a cryptographic unit are set to state pre-activation. Keys generated by cryptographic units are never considered in a pre-activation state.
- **Active** – state 1 – After KMS service generates or stores a key from a cryptographic unit, it is set to the Active state.
- **Tainted** – state 2 – The P1619.3 state specifying a key that has been requested and allowed to be used by a cryptographic unit that did not meet the security requirements of the key. The key is still usable for both encrypt and decrypt processes.
- **Deactivated** – state 3 – A key that is used to decrypt only will be set to the deactivated state. This function must be configurable by a group manager via time stamp or
- **Compromised** – state 4 – A key that has potentially been compromised but must be available for decryption by an authorized CU will be set to the compromised state. This state allows for a key to be used only to decrypt data. This state must be honored by cryptographic units in order to be enforced.
- **Disabled** – state 5 – This state applies specifically to data at rest. This state defines a key that has been destroyed on all cryptographic units and only exists in the KMS service but is not accessible by any KM Client. Keys can be transitioned directly from active to disallow use by cryptographic units in cases where the media has been lost or stolen. A KM User can transition the key back to a deactivated state or the disabled compromised state depending on why the key was disabled in the first place.
- **Disabled Compromised** – state 6 – Keys that have been compromised at some point during their current lifecycle can be moved to this state either directly from compromised or from the disabled state. This includes discovery that they may have been compromised after they were disabled.
- **Key Zeroed** – state 7 – The Zeroed state denotes a key that is up for removal from the system. Keys that are zeroed still have all other metadata and time stamps left in place. This state keeps a key from being imported back into the system that may have been exported, backed up or stored elsewhere.
- **Key Zeroed Compromised** – state 8 – This state denotes keys that were compromised then destroyed or destroyed and then discovered to be compromised.
- **Key Purged** – state 9 – When the key record (metadata) is no longer required it may be purged by the system to release the SO_GUID and Record ID for reuse. Only the zeroed key and the associated metadata are deleted. All logged information about the key must still be maintained.

Use Figure 1 to show the key states and their associated transitions.

Key State Transitions

Using the below diagram the following defines the different transitions that are required with the new set of key states.

Figure 1 - Key State Transition Diagram



Transition 1: When a key is generated within a KMS system, but not returned to the cryptographic unit it is placed in the Pre-Activation state. Keys that are generated by cryptographic units stored in a KM Server are placed immediately in the Active state.

Transition 2: It must be possible for a key to be moved directly from Pre-Activation to Key Record Purged. If key has never been active but is no longer required the entire record can be purged since there is no requirement for information pertaining to that key other than log information that it was created and purged.

Transition 3: When a Pre-Activated state key is requested by a KM Client it transitions to the Active state. If a key is exported singly, as part of a SO_Context or as part of a SO_Domain it must be transitioned to Active.

Transition 4: Active keys that have potentially been exposed or are considered compromised will transition to the Compromised state.

Transition 5: If a key is expired and no longer required for use it may be transitioned directly to Disabled state. This applies for symmetric keys that have an associated expiration.

- Transition 6:** Keys that are only to be used to decrypt information are transitioned to the Deactivated state. Devices that do not support decrypt only functions are not to have keys returned to them.
- Transition 7:** If a key has a minimum security level set and a device is allowed to request the key that does not meet that security level a key will be transitioned to Tainted.
- Transition 8:** Keys that are in a Tainted state and can still be used to decrypt only move to Compromised state. Tainted keys can only move to a Compromised state as the security level required for the key was not met at some point in its lifecycle.
- Transition 9:** Keys that have been deactivated for decryption only that are used by devices with lower security levels than required, potentially exposed or have been exposed but are still required for use are transitioned to the Compromised state.
- Transition 10:** Deactivated keys that are no longer required for any use are transited to the Disabled state.
- Transition 11:** If a key that has been compromised is no longer required it will be moved to the Disable Compromised State.
- Transition 12:** Keys that are required for use again may be restored for decrypt only purposes to the Deactivated state.
- Transition 13:** Keys that are in the Disabled Compromised state may be returned to use as Compromised for decryption only operations.
- Transition 14:** Keys that are disabled that have or may have been exposed during the accessible stages of their lifecycle or after they are disabled are transitioned to the Disabled Compromised state.
- Transition 15:** Once a key has been disabled and there is no requirement for it to exist anymore, the keying material may be zeroed while the rest of the key’s metadata still exists. The key is transitioned to the Key Zeroed state.
- Transition 16:** Keys that are Disabled Compromised being zeroed are moved to the Key Zeroed Compromised state.
- Transition 17:** Keys that are found to have been exposed during their existence in a Key Zeroed state may be moved to Key Zeroed Compromised state.
- Transition 18:** When all information regarding a specific key is no longer required the metadata and zeroed key may be purged from the system completely. This may include ensuring that This will free the SO_GUID and the Record ID for use again. Logging information pertaining to the key must still be maintained even after deletion.
- Transition 19:** Key Zeroed Compromised keys that are no longer required can also be purged once the record is no longer required.

Comparison of NIST Key States and Proposed Key States

The following are the mappings from the new key states to the NIST SP800-57 states:

Table 1 – Proposed State to NIST State Mapping

Proposed State	NIST SP800-57 State	Notes
Pre-Activation	Pre-Activation	Identical state for proposed state and NIST SP800-57
Active	Active	Identical state for proposed state and NIST SP800-57
Tainted	--	Tainted allows the key to still be used for encryption. NIST does not have an equivalent state as Tainted.

Proposal for P1619.3 Key State

Proposed State	NIST SP800-57 State	Notes
Deactivated	Deactivated	Allows use of key for decryption only. Identical state for proposed state and NIST SP800-57
Compromised	Compromised	Identical state for proposed state and NIST SP800-57
Disabled	--	Proposed state only. Used for Symmetric keys that is removed from service but may be returned to the deactivated state in special cases.
Disabled Compromised	--	Proposed only state. Used for Symmetric keys that is removed from service but may be returned to the compromised state in special cases.
Key Zeroed	Destroyed	Proposed state Key Zeroed applies only to keying material and not to associated metadata.
Key Zeroed Compromised	Destroyed Compromised	Proposed Key Zeroed Compromised state applies only to keying material and not to associated metadata of keys that have been compromised.
Key Purged	Destroyed / Destroyed Compromised	Applies to all keying material and associated metadata. Logged information about the key is still available to KM Users