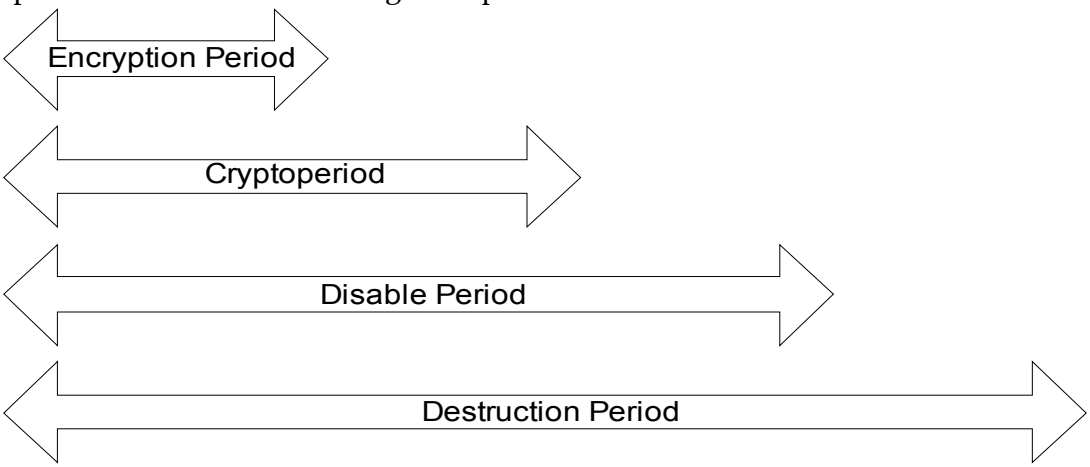
Proposed P1619.3 Key Life Cycle

11/19/2007

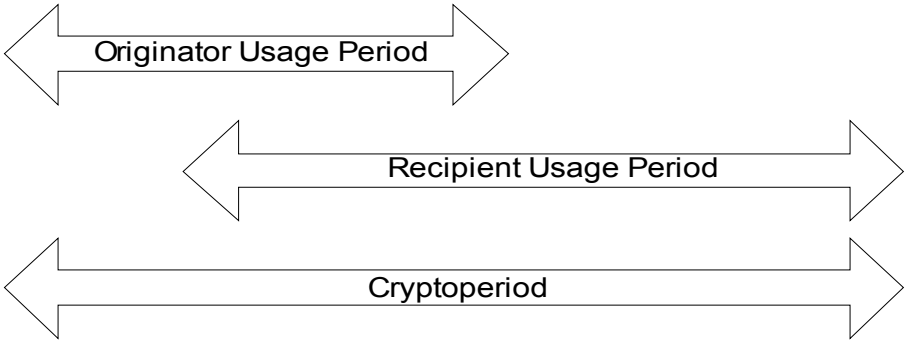
Key Life Cycle

This life cycle is based on the NIST 800-57 guidelines. A few additional states are added.

The key life cycle is based on four time periods. These are the encryption period, cryptoperiod, disable period, and destruction period. All periods start when a key is activated. This occurs when a key is given to a KM Client by a KM Server, or when a key generated by a KM Client is given to the KM Server. The encryption period is the period of time after a key is activated that it can be used to encrypt data. The cryptoperiod is the time period it can be used for routine decryption. The disable period is the period of time before a key will be disabled and become unavailable to clients. A key may still be delivered to a KM Client after the cryptoperiod ends but before the disable period ends. This would be for a non-routine usage of the key. The destruction period is the period of time before the key is destroyed by the KM Server. Any time period can range from zero to forever, with the limitation that each time period must be at least as long as its predecessor.



The first two time periods are a simplification from NIST's terminology and from the NIST approach of two time periods that may be offset. NIST defines the “originator usage period” and “recipient usage period”.



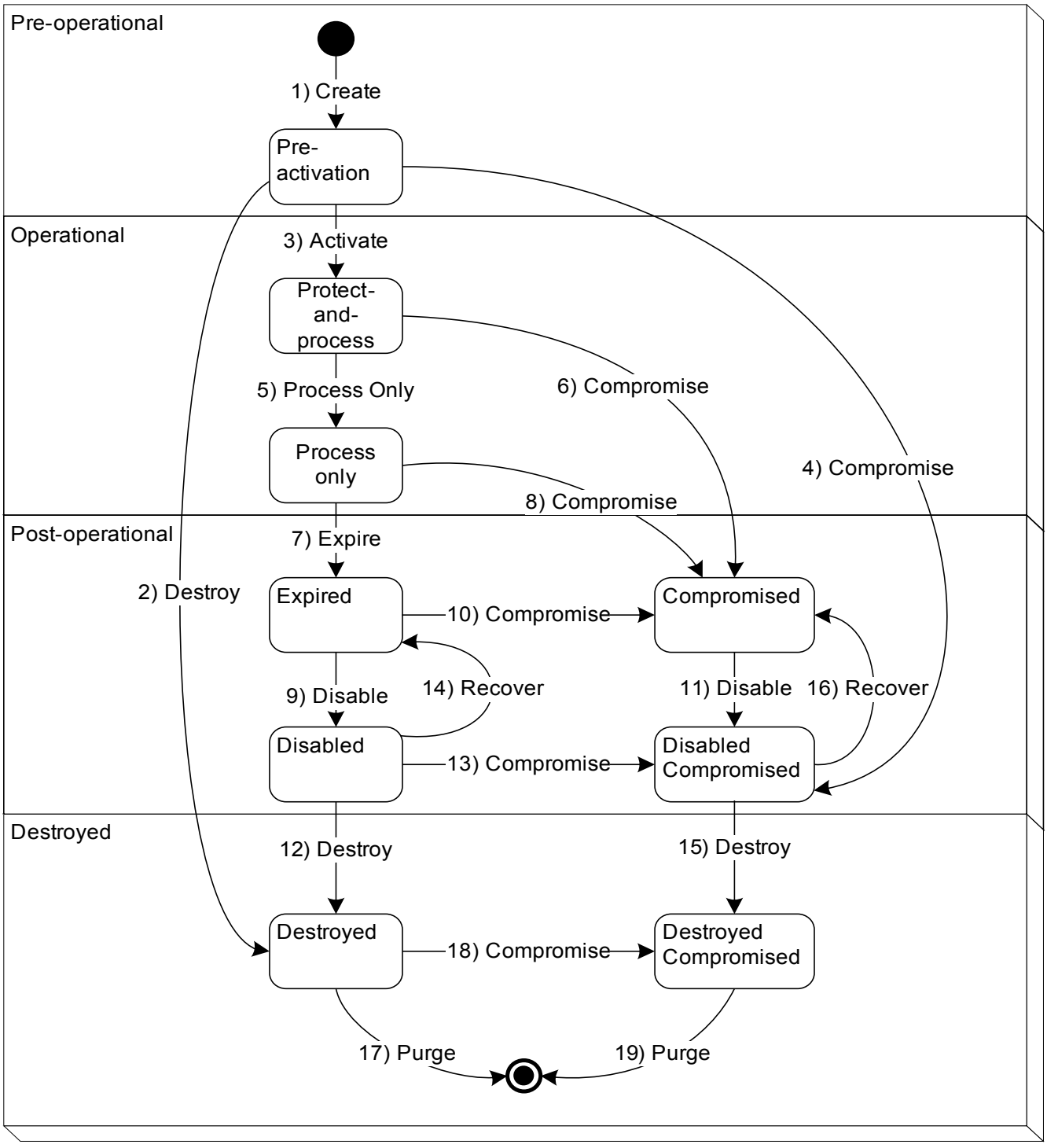
The originator usage period is the same as the encryption period above. The recipient usage period may start after the originator usage period. Since storage devices may need to read data implicitly as soon as its written, the simplified approach above is used. Therefore, the simplified diagram is more appropriate for stored data encryption keys.

The last two time periods are not explicitly defined in NIST 800-57.

These time periods will cause the KM Server to automatically transition keys from one state to another as time passes. These same transitions, as well as non-timed transitions, may also be caused by user actions on the KM Server.

Key State Diagram

These time periods, combined with other functions of the key manager define a state transition diagram for keys:



The large, square-cornered boxes are the NIST 800-57 phases.

Key States

Pre-activation

The key has generated but is not yet in use or distributed to any KM Client or Cryptographic Unit. A key in this state can only exist in the KM Server. Such a key can be distributed to a KM Client.

Protect-and-process

A key in this state can be used for both encryption (i.e., to protect information) and decryption (to process information). A key is placed into this state when it is initially given to a KM Client, i.e., it is activated. The activation is done when a KM Client requests a new key. If a key is created by a KM Client or Cryptographic Unit and is then given to the KM Server, the key will be immediately placed into protect-and-process state. A key will remain in this state until the encryption period passes.

Process only

A key in this state can be used for decryption but not encryption. When a KM Client/Cryptographic Unit determines that none of the keys available to it (e.g., for a specific tape cartridge or disk volume that is being read or written) are in the protect-and-process state, and it needs to perform encryption, it should create a new key. Keys transition from protect-and-process to process when the encryption period for the key expires, or as a result of an administrative action. A key will remain in the process only state until the cryptoperiod passes. At that time the key will be expired and move to the expired state.

Expired

An expired key is a key that has passed its cryptoperiod. It may still be needed to process (decrypt) information. NIST specifically states that keys in this state may be used to process data. An expired key will be delivered to a KM Client, but the Cryptographic Unit should not use the key to encrypt data. A key will remain in this state until the disable period passes or as a result of an administrative action. At that time the key will be disabled and move to the disabled state.

The difference between process only and expired keys is subtle. As far a KM Clients or Cryptographic Units are concerned, the states are equivalent. The difference is significant only to KM Servers. A process only key is still in the NIST operational phase, and would routinely be delivered to KM Clients. An expired key has moved into the NIST post-operational phase, and may have additional restrictions imposed on its delivery to KM Clients.

Disabled

A disabled key is a key that is still known to the KM Server but that will not be delivered to a KM Client. The key material remains intact in the KM Server for a disabled key. A key will remain in the disabled state until the destruction period expires. At that time, the key will be destroyed and move to the destroyed state.

Compromised

Keys are compromised when they are released to or discovered by an unauthorized entity. Compromised keys should not be used to protect information, but may need to be used to process information. The KM server cannot determine if a key has been compromised. An administrative action is needed to inform a KM server that a key has been compromised. A compromised key will be delivered to a KM Client, but the Cryptographic Unit should not use the key to encrypt data. As for Expired keys, a KM Server may impose additional restrictions on the delivery of compromised keys to a KM Client. A key will remain in this state until the disable period passes. At that time the key will be disabled and move to the disabled compromised state.

Disabled Compromised

A key that is both disabled and compromised. Disabled compromised keys will never be delivered to KM Clients. A key will remain in the disabled compromised state until the destruction period expires. At that time, the key will be destroyed and move to the compromised destroyed state.

Destroyed

A destroyed key is a key who's key material has been removed from the KM Server. Information or metadata about the key may be retained by the KM Server. Destroyed keys will have their key material removed from the KM Server. Destroyed keys cannot be delivered to a KM Client. The only way to destroy a key is via an administrative action in the KM Server. The NIST guidelines do not appear to provide any basis for destroying keys based on time. The standard allows for time based key destruction based on the destruction period.

Destroyed Compromised

Same as destroyed, but the key was compromised before or after destruction.

Terminal (Purged)

Purged is the terminal state for keys. A purged key is a key that no longer exists in the KM Server in any form. Neither the key material nor any metadata about the key is known to the KM Server. A purged key cannot be delivered to a KM Client.

State Transitions

1) Create

When a key is created by a KM Server, it begins in the pre-activation state. This transition occurs as soon as a key is generated within the KM Server, such as a key being generated by a RNG.

Transition 1 applies to newly created keys. The key transitions to pre-activation state.

2) Destroy

A pre-activation state key may be moved directly from pre-activation state to destroyed state. If the

key has never been activated and is no longer required, but there is a requirement to maintain information about the key, the key may be destroyed.

Transition 2 applies to pre-activation keys. The key transitions to destroyed state.

3) Activate

A key transitions from pre-activation to protect-and-process when it is available for use. This transition occurs when the key is assigned for use by a KM Client. There is a bit of confusion around the terminology, since a KM Client may view this action as "creating a key" even though the KM Server views this as assigning a previously generated key.

Transition 3 applies to pre-activation keys. The key transitions to protect-and-process state.

4) Compromise

A key transitions to compromised state when it has been determined to have been released to or discovered by an unauthorized entity. The KM Server cannot determine that this has happened, so this transition occurs as the result of an administrative action.

Transition 4 applies to pre-activation keys. The key transitions to Compromised state.

5) Process Only

A key transitions from the protect-and-process state when a period of time equal the encryption period has passed after the key is activated. This transition may also occur as a result of administrative action. Some KM Clients and Cryptographic Units may be unable to strictly enforce this transition.

Transition 5 applies to protect-and-process keys. The key transitions to process only state.

6) Compromise

Same actions as for 4) Compromise.

Transition 6) applies to protect-and-process keys. The key transitions to compromised state.

7) Expire

A key transitions from active to Expired when its cryptoperiod expires. This transition may also occur as a result of administrative action.

NIST defines two other situations where this transition can occur. These are "key update" as described in 8.2.3.2 on page 106 and key revocation for reasons other than compromise as described in 8.3.5 on page 112. These situations are not covered by this diagram or by the standard. The standard does not provide for a key having more than one key value, so the concept of updating a key (i.e., giving an existing key a new value) does not apply. The standard does not cover key revocation for reasons other than compromise.

Transition 7 applies to process only keys. The key transitions to expired state.

8) Compromise

Same actions as for 4) Compromise.

Transition 8) applies to process only keys. The key transitions to compromised state.

9) Disable

This transition will occur after the disable period for a key passes. This transition can also occur as a result of administrative actions. The key material and its metadata will be retained by the KM Server. The key will no longer delivered to KM Clients.

Transition 9 applies to expired keys. The key will transition to disabled state.

10) Compromise

Same actions as for 4 Compromise.

Transition 10 applies to expired keys. The key transitions to compromised state.

11) Disable

Same actions as for 9 Disable

Transition 11 applies to compromised keys. The key transitions to disabled compromised state.

12) Destroy

A key can be destroyed when it is no longer needed. When the destruction period for a key passes, it will be destroyed. This transition can also occur as a result of administrative action. Active keys cannot be destroyed, per the NIST state diagrams. When a key is destroyed, the key material is removed from the KM Server. Metadata about the key is retained in the KM Server

Transition 12 applies for destroying disabled keys. The key transitions to destroyed state.

13) Compromise

Same actions as for 4 Compromise.

Transition 13 applies to disabled keys. The key transitions to disabled compromised state.

14) Recover

When a disabled key is required to be delivered to KM Clients, it can be recovered. This occurs as a result of an administrative action.

Transition 14 applies to disabled keys. The key is transitions to expired state.

15) Destroy

Same actions as for 12 Destroy.

Transition 15 applies to destroying a disabled compromised key. The key transitions to destroyed compromised state.

16) Recover

Same actions as for 14 Recover.

Transition 20 applies to disabled compromised keys. The key transitions to compromised state.

17) Purge

The action of purging a key removes all information about the key from the KM Server's key records. Neither the key material nor the key value will be retained by the KM Server. Note, however, that audit logs or other indirect information in the KM Server may still contain information about the key.

Transition 17 applies to destroyed keys. The key transitions to purged state. However, since the key does not exist in the KM Server, there is no record for the key showing the purged state.

18) Compromise

Same actions as for 4) Compromise.

Transition 18) applies to destroyed keys. The key transitions to destroyed compromised state.

19) Purge

Same actions as for 17 Purge

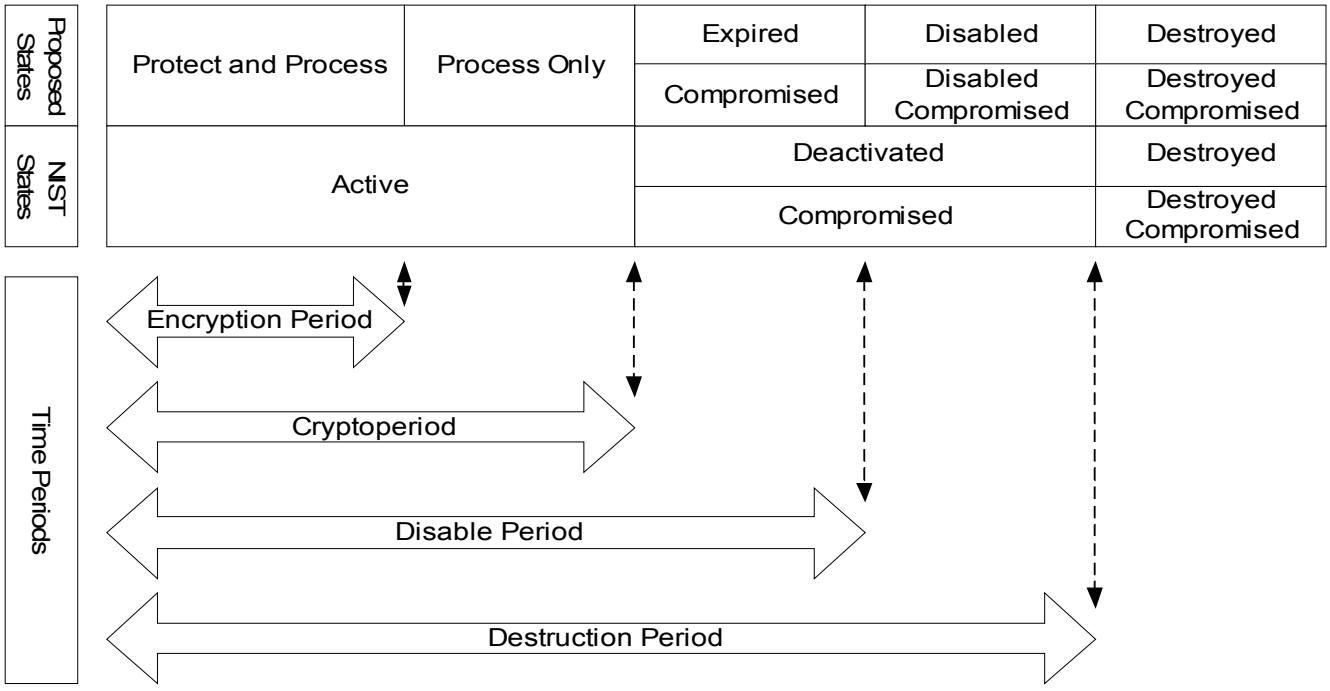
Transition 19 applies to destroyed compromised keys. The key transitions to purged state. However, since the key does not exist in the KM Server, there is no record for the key showing the purged state.

Comparison of NIST Key State and Proposed Key States

The following are the mappings from the proposed key state to the NIST 800-57 key states

Proposed State	NIST 800-57 State	Notes
Pre-activation	Pre-activation	Identical
Protect-and-process	Active	Proposed state is a more detailed substate of NIST 800-57 state
Process only	Active	Proposed state is a more detailed substate of NIST 800-57 state
Expired	Deactivated	Proposed state is a substate of NIST 800-57 state.
Disabled	Deactivated	Proposed state is a substate of NIST 800-57 state.
Compromised	Compromised	Proposed state is a substate of NIST 800-57 state.
Disabled Compromised	Compromised	Proposed state is a substate of NIST 800-57 state.
Destroyed	Destroyed	Identical
Destroyed Compromised	Destroyed Compromised	Identical
Purged	None	New state not defined in NIST 800-57.

The diagram below shows graphically how the proposed state, the NIST state, and the time periods correlate:



Comparison of ISO Key State and Proposed Key States

The following are the mappings from the proposed key state to the ISO 11770 standard

Proposed State	ISO 11770 State	Notes
Pre-activation	Pending Active	Identical
Protect-and-process	Active	Proposed state is a more detailed substate of ISO 11770 state
Process only	Active	Proposed state is a more detailed substate of ISO 11770 state
Expired	Deactivated	Proposed state is a substate of ISO 11770 state.
Disabled	Deactivated	Proposed state is a substate of ISO 11770 state.
Compromised	None	New state not defined in ISO 11770.
Disabled Compromised	None	New state not defined in ISO 11770.
Destroyed	Destroyed (Implied)	Same as destroyed state implied in ISO 11770.
Destroyed Compromised	None	New state not defined in ISO 11770.
Purged	None	New state not defined in ISO 11770.