NIST Req #	NIST 800-130 Requirement Text	Evernym Classification	Digital Bazaar Classification		Same	Modified	N/A	Total
FR:1.1	A conformant CKMS design shall meet all “shall” requirements of the Framework.	Same	Same		1			1
	Framework Basics				4	1	0	5
FR:2.1	The CKMS design shall specify all cryptographic algorithms and supported key sizes for each algorithm used by the system.	Same	Same					
FR:2.2	The CKMS design shall specify the estimated security strength of each cryptographic technique that is employed to protect keys and their bound metadata.	Same	Same					
FR:2.3	A compliant CKMS design shall describe design selections and provide documentation as required by the requirements of this Framework.	Same	Same					
FR:2.4	The CKMS design shall specify a high-level overview of the CKMS system that includes: a) The use of each key type, b) Where and how the keys are generated, c) The metadata elements that are used in a trusted association with each key type, d) How keys and/or metadata are protected in storage at each entity where they reside, e) How keys and/or metadata are protected during distribution, and f) The types of entities to which keys and/or metadata can be delivered (e.g., user, user device, network device).	Same	Same					
FR: 2.5	The CKMS design shall specify all major devices of the CKMS (e.g., the make, model, and version).	**Modify**	N/A					
	Goals				6	7	3	16
FR:3.1	The CKMS design shall specify its goals with respect to the communications networks on which it will function.	Same	Same					
FR:3.2	The CKMS design shall specify the intended applications that it will support.	**Modify**	Same					
FR:3.3	The CKMS design shall list the intended number of users and the responsibilities that the CKMS places on those users.	**Modify**	N/A					
FR:3.4	The CKMS design shall specify the COTS products used in the CKMS.	N/A	N/A					
FR:3.5	The CKMS design shall specify which security functions are performed by COTS products.	N/A	N/A					
FR:3.6	The CKMS design shall specify how COTS products are configured and augmented to meet the CKMS goals.	N/A	N/A					
FR:3.7	The CKMS design shall specify the Federal, national, and international standards that are utilized by the CKMS.	Same	Same					
FR:3.8	For each standard utilized by the CKMS, the CKMS design shall specify which CKMS devices implement the standard.	**Modify**	N/A					
FR:3.9	For each standard utilized by the CKMS, the CKMS design shall specify how conformance to the standard was validated (e.g., by a third party testing program).	**Modify**	Modify					
FR:3.10	The CKMS design shall specify all user interfaces to the system.	**Modify**	N/A					
FR:3.11	The CKMS design shall specify the results of any user-acceptance tests that have been performed regarding the ease of using the proposed user interfaces.	Same	N/A					
FR:3.12	The CKMS design shall specify the design principles of the user interface.	Same	Modify					
FR:3.13	The CKMS design shall specify all human error-prevention or failsafe features designed into the system.	**Modify**	Same					
FR:3.14	The CKMS design shall specify the performance characteristics of the CKMS, including the average and peak workloads that can be handled for the types of functions	Same	Same					
FR:3.15	The CKMS design shall specify the techniques that are supported and can be used to scale the system to increased workload demands.	Same	Same					
FR:3.16	The CKMS design shall specify the extent to which the CKMS can be scaled to meet increased workload demands. This shall be expressed in terms of additional workload, response times for the workload, and cost.	Same	Same					
	Security Policies				22	5	0	27
FR:4.1	The CKMS design shall specify the CKMS Security Policy, including the configurable options and sub-policies that it is designed to enforce.	**Modify**	Same					
FR:4.2	The CKMS design shall specify how the CKMS Security Policy is to be enforced by the CKMS (e.g., the mechanisms used to provide the protection required by the policy).	**Modify**	Same					
FR:4.3	The CKMS design shall specify how any automated portions of the CKMS Security Policy are expressed in an unambiguous tabular form or a formal language (e.g., XML or ASN.1), such that an automated security system (e.g., table driven or syntax- directed software mechanisms) in the CKMS can enforce them.	Same	Same					
FR:4.4	The CKMS design shall specify other related security policies that support the CKMS Security Policy.	**Modify**	Same					
FR:4.5	The CKMS design shall specify the policies that are supported by the CKMS design and a summary of how they are supported by the design.	**Modify**	Same					
FR:4.6	The CKMS design shall specify if and how personal accountability is supported by the CKMS.	Same	Same					
FR:4.7	The CKMS design shall specify the anonymity, unlinkability, and unobservability policies that can be supported by the CKMS.	Same	Same					
FR:4.8	The CKMS design shall specify which CKMS transactions have or can be provided with anonymity protection.	Same	Same					
FR: 4.9	The CKMS design shall specify how CKMS transaction anonymity is achieved when anonymity assurance is provided.	Same	Same					
FR:4.10	The CKMS design shall specify which CKMS transactions have or can be provided with unlinkability protection.	Same	Same					
FR:4.11	The CKMS design shall specify how CKMS transaction unlinkability is achieved.	Same	Same					
FR:4.12	The CKMS design shall specify which CKMS transactions have or can be provided with unobservability protection.	Same	Same					
FR:4.13	The CKMS design shall specify how CKMS transaction unobservability is achieved.	Same	Same					
FR:4.14	The CKMS design shall specify the countries and/or regions of countries where it is intended for use and any legal restrictions that the CKMS is intended to enforce.	**Modify**	Modify					
FR:4.15	The CKMS design shall specify design features that allow for the exchange of keys and metadata with entities in other security domains that are considered to offer equivalent but different security protections.	Same	Same					
FR:4.16	The CKMS design shall specify the source and destination authentication policies that it enforces when sharing a key and/or metadata with entities in differing security domains.	Same	Same					
FR:4.17	The CKMS design shall specify the confidentiality and integrity policies that it enforces when sharing a key and/or metadata with entities in differing security domains.	Same	Same					
FR:4.18	The CKMS design shall specify what assurances it requires when communicating with entities from other security domains.	Same	Same					
FR:4.19	The CKMS design shall specify if and how it supports the review and verification of another domain’s security before intra-domain communications are permitted.	Same	Same					
FR: 4.20	The CKMS design shall specify how it detects, prevents or warns an entity of the possible security consequences of communicating with an entity in a security domain with weaker policies.	Same	Same					

NIST Req #	NIST 800-130 Requirement Text	Evernym Classification	Digital Bazaar Classification		Same	Modified	N/A	Total
FR:4.21	The CKMS design shall specify whether or not it supports multilevel security domains.	Same	Same					
FR:4.22	The CKMS design shall specify each level of security domain that it supports.	Same	Same					
FR:4.23	If multilevel security domains are supported, the CKMS design shall specify how it maintains the separation of the keys and metadata belonging to each security level.	Same	Same					
FR:4.24	The CKMS design shall specify if and how it supports the upgrading or downgrading of keys and metadata.	Same	Same					
FR:4.25	The CKMS design shall specify how upgrading or downgrading capabilities are restricted to the domain authority.	Same	Same					
FR:4.26	The CKMS design shall specify if and how its key and/or metadata management functions may be configured to support differing domain security policies and differing applications.	Same	Same					
FR:4.27	The CKMS design shall specify if and how it can support changes in its Domain Security Policy by being reconfigured to accommodate communications with entities in different security domains.	Same	Same					
	Roles and Responsibility				4	1	0	5
FR:5.1	The CKMS design shall specify each role employed by the CKMS, the responsibilities of each role, and how entities are assigned to each role.	Same	Same					
FR:5.2	The CKMS design shall specify the key and metadata management functions (see Section 6.4) that can be used by entities fulfilling each role employed by the CKMS.	Same	Same					
FR:5.3	The CKMS design shall specify which roles require role separation.	Same	Same					
FR:5.4	The CKMS design shall specify how the role separation is maintained for the roles that require role separation.	Same	Same					
FR:5.5	The CKMS design shall specify all automated provisions for identifying security violations, whether by individuals performing authorized roles (insiders) or by those with no authorized role (outsiders).	**Modify**	Same					
	Cryptographic Keys and Metadata				76	45	3	124
FR:6.1	The CKMS design shall specify and define each key type used.	**Modify**	Same					
FR:6.2	For each key type used in the system, the CKMS design shall specify all metadata elements selected for a trusted association, the circumstances under which the metadata elements are created and associated with the key, and the method of association (i.e., cryptographic mechanism or trusted process).	Same	Same					
FR:6.3	For each cryptographic mechanism used in the Key Protections metadata element (item s) above--see page 34), the CKMS design shall specify the following: i. The cryptographic algorithm: See item g) above. (PDF page 32) ii. The parameters for the key: See item i) above. (PDF page 33) iii. The key identifier: See item b) above. (PDF page 32) iv. The protection value: This element contains the protection value for integrity protection, confidentiality protection, or source authentication. For example, a properly implemented MAC or digital signature technique may provide for integrity protection and/or source authentication. v. When the protection was applied. vi. When the protection was verified.	Same	Same					
FR:6.4	For each non-cryptographic trusted process used in the Key Protections metadata element (item s above), the CKMS design shall specify the following: i. The identifier of the process used to distinguish it from other processes, and ii. A description of the process or a pointer to a description of the process.	N/A	N/A					
FR:6.5	For each cryptographic mechanism used in the Metadata Protections metadata element (item t above--PDF page 35), the CKMS design shall specify the following: i. The cryptographic algorithm. ii. The parameters for the key. iii. The key identifier. iv.The protection value (e.g., MAC, digital signature). v. When the protection was applied. vi. When the protection was verified.	Same	Same					
FR:6.6	For each non-cryptographic trusted process used in the Metadata Protections metadata element (item t above--PDF page 35), the CKMS design shall specify the following: i. The identifier that is used to distinguish this process from other processes, and ii. A description of the process or a pointer to a description of the process.	N/A	N/A					
FR:6.7	For each cryptographic mechanism used in the Trusted Association Protections metadata element (item u) above--PDF page 35), the CKMS design shall specify the following: i. The cryptographic algorithm, ii. The parameters for the key, iii. The key identifier, iv. The protection value (e.g., MAC, digital signature), v. When the protection was applied, and vi. When the protection was verified.	Same	Same					
FR:6.8	For each non-cryptographic trusted process used in the Trusted Association Protections metadata element (item u) above--PDF page 35), the CKMS design shall specify the following: i. The identifier that is used to distinguish this process from other processes, and ii. A description of the process or a pointer to a description of the process.	N/A	N/A					
FR:6.9	The CKMS design shall specify the accuracy and precision required for dates and times used by the system.	Same	Same					
FR:6.10	The CKMS design shall specify what authoritative time sources are used to achieve the required accuracy.	Same	Same					
FR:6.11	The CKMS design shall specify how authoritative time sources are used to achieve the required accuracy.	Same	Same					
FR:6.12	The CKMS design shall specify which dates, times, and functions require a trusted third-party time stamp.	Same	Same					

NIST Req #	NIST 800-130 Requirement Text	Evernym Classification	Digital Bazaar Classification		Same	Modified	N/A	Total
FR:6.13	For each key type, the CKMS design shall specify the following information regarding keys and metadata elements: a) The key type b) The cryptoperiod (for static keys) c) The method of generation i. The RNG used ii. A key generation specification (e.g., [FIPS 186] for signature keys, [SP 800- 56A] for Diffie-Hellman key establishment keys) d) For each metadata element, include i. The source of the metadata ii. How the metadata is vetted e) The method of key establishment i. The key transport scheme (if used) ii. The key agreement scheme (if used) iii. The protocol name (if a named protocol is used) f) The disclosure protections (e.g., key confidentiality, physical security) g) The modification protections (e.g., a MAC or a digital signature) h) The applications that may use the key (e.g., TLS, EFS, S/MIME, IPSec, PKINIT, SSH, etc.) i) The applications that are not permitted to use the key j) The key assurances i. Symmetric key assurances (e.g., format checks) -Who obtains the assurance -The circumstances under which it is obtained -How the assurance is obtained ii. Asymmetric key assurances (e.g., assurance of possession and validity) -Who obtains the assurances -The circumstances under which the assurance is obtained -How the assurance is obtained iii. Domain parameter validity checks -Who performs the validity check -The circumstances under which the checking is performed -How the assurance of domain parameter validity was obtained.	**Modify**	Modify					
FR:6.14	The CKMS design shall specify all syntax, semantics, and formats of all key types and their metadata that will be created, stored, transmitted, processed, and otherwise managed by the CKMS.	**Modify**	Modify					
FR:6.15	The CKMS design shall specify all the states that the CKMS keys can attain.	Same	Same					
FR:6.16	The CKMS design shall specify all transitions between the CKMS key states and the data (inputs and outputs) involved in making the transitions.	Same	Same					
FR:6.17	The CKMS design shall specify the key and metadata management functions to be implemented and supported.	Same	Same					
FR:6.18	The CKMS design shall identify the integrity, confidentiality, and source- authentication services that are applied to each key and metadata management function parameter implemented in the CKMS.	**Modify**	Modify					
FR:6.19	The CKMS design shall specify the key-generation methods to be used in the CKMS for each type of key.	**Modify**	Modify					
FR:6.20	The CKMS design shall specify the underlying random number generators that are used to generate symmetric and private keys.	**Modify**	N/A					
FR:6.21	The CKMS design shall specify all the processes involved in owner registration, including the process for binding keys with the owner's identifier.	**Modify**	Same					
FR:6.22	The CKMS design shall specify how each key type is activated and the circumstances for activating the key.	**Modify**	Modify					
FR:6.23	For each key type, the CKMS design shall specify requirements for the notification of key activation, including which parties are notified, how they are notified, what security services are applied to the notification, and the time-frames for notification(s).	**Modify**	Modify					
FR:6.24	The CKMS design shall specify for each key type how deactivation of the key is determined (e.g., by cryptoperiod, by number of uses, or by amount of data).	Same	Same					
FR:6.25	The CKMS design shall specify how each key type is deactivated (e.g., manually or automatically, based on the deactivation date-time, the number of usages, or the amount of protected data).	Same	Same					
FR:6.26	The CKMS design shall specify how the deactivation date-time for each key type can be changed.	Same	Same					
FR:6.27	For each key type, the CKMS design shall specify requirements for advance notification of the deactivation of the key type, including which CKMS supported roles are notified, how they are notified, what security services are applied to the notification, and the time-frames for notification(s).	Same	Same					
FR:6.28	The CKMS design shall specify when, how, and under what circumstances revocation is performed and revocation information is made available to the relying parties.	Same	Same					
FR:6.29	The CKMS design shall specify how, and under what circumstances, a key is suspended.	Same	Same					
FR:6.30	The CKMS design shall specify how suspension information is made available to the relying or communicating parties.	Same	Same					
FR:6.31	The CKMS design shall specify how, and under what circumstances, a suspended key is re-activated.	Same	Same					
FR:6.32	The CKMS design shall specify how the suspended key is prevented from performing security services.	Same	Same					
FR:6.33	The CKMS design shall specify how re-activation information is made available to the relying or communicating parties.	Same	Same					
FR:6.34	The CKMS design shall specify how and the conditions under which a public key can be renewed.	Same	Same					
FR:6.35	For each key type, the CKMS design shall specify requirements for advance notification of the renewal of the key type, including which parties are notified, how they are notified, what security services are applied to the notification, and the time-frames for notification(s).	Same	Same					
FR:6.36	The CKMS design shall specify all processes used to derive or update keys and the circumstances under which the keys are derived or updated.	Same	Same					
FR:6.37	For each key type, the CKMS design shall specify requirements for advance notification of the derivation or update of the keys, including which parties are notified, how they are notified, what security services are applied to the notification, and the time- frames for notification(s).	Same	Same					
FR:6.38	The CKMS design shall specify how and the circumstances under which keys are intentionally destroyed and whether the destruction is local to a component or universal throughout the CKMS.	Same	Same					
FR:6.39	For each key type, the CKMS design shall specify requirements for an advance notification of key destruction, including which parties are notified, how they are notified, what security services are applied to the notification, and the time-frames for notification(s).	Same	Same					
FR:6.40	For each key type used, the CKMS design shall specify what metadata is associated with the key, how the metadata is associated with the key, and the circumstances under which metadata is associated with the key.	Same	Same					
FR:6.41	For each key type used, the CKMS design shall describe how the following security services (protections) are applied to the associated metadata: source authentication, integrity, and confidentiality.	Same	Same					
FR:6.42	The CKMS design shall specify the circumstances under which associated metadata is modified.	Same	Same					
FR:6.43	The CKMS design shall specify the circumstances under which the metadata associated with a key is deleted.	Same	Same					

NIST Req #	NIST 800-130 Requirement Text	Evernym Classification	Digital Bazaar Classification		Same	Modified	N/A	Total
FR:6.44	The CKMS design shall specify the technique used to delete associated metadata.	Same	Same					
FR:6.45	For each key type, the CKMS design shall specify which metadata can be listed by authorized entities.	Same	Same					
FR:6.46	For each key type, the CKMS design shall specify: the circumstances under which keys of each type and their metadata are stored, where the keys and metadata are stored, and how the keys and metadata are protected.	**Modify**	Modify					
FR:6.47	The CKMS design shall specify how, where, and the circumstances under which keys and their metadata are backed up.	**Modify**	Modify					
FR:6.48	The CKMS design shall specify the security policy for the protection of backed- up keys/metadata.	**Modify**	Modify					
FR:6.49	The CKMS design shall specify how the security policy is implemented during the key and metadata back-up, e.g., how the confidentiality and multi-party control requirements are implemented during transport and storage of the backed-up keys and metadata.	**Modify**	Modify					
FR:6.50	The CKMS design shall specify how, where, and the circumstances under which keys and/or their metadata are archived.	**Modify**	Modify					
FR:6.51	The CKMS design shall specify the technique for the secure destruction of the key and/or metadata or the secure destruction of the old storage medium after being written onto a new storage medium.	**Modify**	Modify					
FR:6.52	The CKMS design shall specify how keys and/or their metadata are protected after the cryptoperiod of an archive key expires.	**Modify**	Modify					
FR:6.53	The CKMS design shall specify the CKMS recovery policy for keys and/or metadata.	**Modify**	Same					
FR:6.54	The CKMS design shall specify the mechanisms used to implement and enforce the recovery policy for keys and/or metadata.	**Modify**	Same					
FR:6.55	The CKMS design shall specify how, and the circumstances under which, keys and/or metadata are recovered from each key database or metadata storage facility.	**Modify**	Modify					
FR:6.56	The CKMS design shall specify how keys and/or metadata are protected during recovery.	**Modify**	Modify					
FR:6.57	The CKMS design shall specify how, and the circumstances under which, keys and their metadata are established.	Same	Same					
FR:6.58	The CKMS design shall specify how, and the circumstances under which, keys and metadata are entered into a cryptographic module, the form in which they are entered, and the method used for entry.	**Modify**	Modify					
FR:6.59	The CKMS design shall specify how the integrity and confidentiality (if necessary) of the entered keys and metadata are protected and verified upon entry.	**Modify**	Modify					
FR:6.60	The CKMS design shall specify how, and the circumstances under which, keys and metadata are output from a cryptographic module and the form in which they are output.	**Modify**	Modify					
FR:6.61	The CKMS design shall specify how the confidentiality and integrity of the output keys and metadata are protected while outside of a cryptographic module.	**Modify**	Modify					
FR:6.62	If a private key, symmetric key, or confidential metadata is output from the cryptographic module in plaintext form, the CKMS design shall specify if and how the calling entity is authenticated before the key and metadata are provided.	**Modify**	Modify					
FR:6.63	The CKMS design shall specify how, where, and the circumstances under which, public key domain parameters are validated.	Same	Same					
FR:6.64	The CKMS design shall specify how, where, and the circumstances under which, public keys are validated.	Same	Same					
FR:6.65	The CKMS design shall specify how, where, and the circumstances under which, a key certification path are validated.	Same	Same					
FR:6.66	The CKMS design shall specify how, where, and the circumstances under which, symmetric keys and/or metadata are validated.	Same	Modify					
FR:6.67	The CKMS design shall specify how, where and the circumstances under which, private keys or key pairs and/or metadata are validated.	Same	Modify					
FR:6.68	The CKMS design shall specify how, where, and the circumstances under which, possession of private keys and their metadata are validated.	Same	Same					
FR:6.69	The CKMS design shall specify all cryptographic functions that are supported and where they are performed in the CKMS (e.g., CA, host, or end user system).	Same	Same					
FR:6.70	The CKMS design shall specify all trust anchor management functions that are supported (see [RFC 6024]).	Same	Same					
FR:6.71	The CKMS design shall specify how the trust anchors are securely distributed so that the relying parties can perform source authentication and integrity verification on those trust anchors.	Same	Same					
FR:6.72	The CKMS design shall specify how the trust anchors are managed in relying- entity systems to ensure that only authorized additions, modifications, and deletions are made to the relying-entity system's trust anchor store.	**Modify**	Modify					
FR:6.73	The CKMS design shall specify the methods used to authenticate the identity and verify the authorization of the entity submitting keys and/or metadata for storage.	Same	Same					
FR:6.74	The CKMS design shall specify the methods used to verify the integrity of keys and/or metadata submitted for storage.	Same	Same					
FR:6.75	The CKMS design shall specify the methods used to protect the confidentiality of symmetric and private stored keys and metadata.	Same	Same					
FR:6.76	If a key wrapping key (or key pair) is used to protect stored keys, then the CKMS design shall specify the methods used to protect the key wrapping key (or key pair) and control its use.	Same	Same					
FR:6.77	The CKMS design shall specify the methods used to protect the integrity of stored keys and metadata.	Same	Same					
FR:6.78	The CKMS design shall specify how access to stored keys is controlled.	Same	Same					
FR:6.79	The CKMS design shall specify the techniques used for correcting or recovering all stored keys.	Same	Same					
FR:6.80	The CKMS design shall specify the methods used to protect the confidentiality of symmetric and private keys during their transport.	Same	Same					
FR:6.81	The CKMS design shall specify the methods used to protect the integrity of transported keys and how the keys can be reconstructed or replaced after detecting errors.	Same	Same					
FR:6.82	The CKMS design shall specify how the identity of the key sender is authenticated to the receiver of transported keying material.	Same	Same					
FR:6.83	The CKMS design shall specify each key agreement scheme supported by the CKMS.	Same	Same					
FR:6.84	The CKMS design shall specify how each entity participating in a key agreement is authenticated.	Same	Same					
FR:6.85	The CKMS design shall specify each key confirmation method used to confirm that the correct key was established with the other entity.	Same	Same					
FR:6.86	The CKMS design shall specify the circumstances under which each key confirmation is performed.	Same	Same					
FR:6.87	The CKMS design shall specify all the protocols that are employed by the CKMS for key establishment and storage purposes.	Same	Same					
FR:6.88	The CKMS design shall specify the topology of the CKMS by indicating the locations of the entities, the ACS, the function logic, and the connections between them.	Same	Same					
FR:6.89	The CKMS design shall specify the constraints on the key management functions that are implemented to assure proper operation.	Same	Same					

NIST Req #	NIST 800-130 Requirement Text	Evernym Classification	Digital Bazaar Classification		Same	Modified	N/A	Total
FR:6.90	The CKMS design shall specify how access to the key management functions is restricted to authorized entities.	Same	Same					
FR:6.91	The CKMS design shall specify the ACS and its policy for controlling access to key management functions.	Same	Same					
FR:6.92	The CKMS design shall specify at a minimum: a) The granularity of the entities (e.g., person, device, organization), b) If and how entities are identified, c) If and how entities are authenticated, d) If and how the entity authorizations are verified, and e) The access control on each key management function.	**Modify**	Same					
FR:6.93	The CKMS design shall specify the capabilities of its ACS to accommodate, implement, and enforce the CKMS Security Policy.	**Modify**	Same					
FR:6.94	The CKMS design shall specify the circumstances under which plaintext secret or plaintext private keys are entered into or output from a cryptographic module.	Same	Same					
FR:6.95	If plaintext secret or plaintext private keys are entered into or output from any cryptographic module, then the CKMS design shall specify how the plaintext keys are protected and controlled outside of the cryptographic module.	Same	Same					
FR:6.96	If plaintext secret or plaintext private keys are entered into or output from any cryptographic module, then the CKMS design shall specify how such actions are audited.	Same	Same					
FR:6.97	For each key and metadata management function, the CKMS design shall specify all human input parameters, their formats, and the actions to be taken by the CKMS if they are not provided.	**Modify**	Same					
FR:6.98	The CKMS design shall specify all functions that require multiparty control, specifying k and n for each function.	**Modify**	Same					
FR:6.99	For each multiparty function, the CKMS design shall cite or specify any known rationale (logic, mathematics) as to why any k of the n entities can enable the desired function, but k−1 of the entities cannot.	**Modify**	Same					
FR:6.100	The CKMS design shall specify all keys that are managed using key splitting techniques and shall specify n and k for each technique.	**Modify**	Same					
FR:6.101	For each (k, n) key splitting technique used, the CKMS design shall specify how key splitting is done, and any known rationale (logic, mathematics) as to why any k of the n key splits can form the key, but k−1 of the key splits provide no information about the key.	Same	Same					
FR:6.102	The CKMS design shall specify the range of acceptable cryptoperiods or usage limits of each type of key used by the system.	Same	Same					
FR:6.103	For each key, a CKMS design shall specify the other key types that depend on the key for their security and how those dependent keys are to be replaced in the event of a compromise of the initial key.	Same	Same					
FR:6.104	The CKMS design shall specify the means by which other compromised keys can be identified when a key is compromised. For example, when a key derivation key is compromised, how are the derived keys determined?	Same	Same					
FR:6.105	For each key type employed, the CKMS design shall specify which metadata elements are sensitive to compromise (confidentiality, integrity, or source).	Same	Same					
FR:6.106	The CKMS design shall specify the potential security consequences, given the compromise (confidentiality, integrity or source) of each sensitive metadata element of a key.	Same	Same					
FR:6.107	The CKMS design shall specify how each sensitive metadata element compromise can be remedied.	Same	Same					
FR:6.108	A CKMS design shall specify the key revocation mechanism(s) and associated relying entity notification mechanism(s) used or available for use.	Same	Same					
FR:6.109	The CKMS design shall specify how physical and logical access to the cryptographic module contents is restricted to authorized entities.	**Modify**	Same					
FR:6.110	The CKMS design shall specify the approach to be used to recover from a cryptographic module compromise.	**Modify**	Same					
FR:6.111	The CKMS design shall describe what non-invasive attacks are mitigated by the cryptographic modules used by the system and provide a description of how the mitigation is performed.	**Modify**	Same					
FR:6.112	The CKMS design shall identify any cryptographic modules that are vulnerable to non-invasive attacks.	**Modify**	Same					
FR:6.113	The CKMS design shall provide the rationale for accepting the vulnerabilities caused by possible non-invasive attacks.	**Modify**	Same					
FR:6.114	The CKMS design shall specify the mechanisms used to detect unauthorized modifications to the CKMS system hardware, software and data.	**Modify**	Same					
FR:6.115	The CKMS design shall specify how the CKMS recovers from unauthorized modifications to the CKMS system hardware, software and data.	**Modify**	Same					
FR:6.116	The CKMS design shall specify how to recover from the compromise of the network security control used by the system. Specifically, a) The CKMS design shall specify the compromise scenarios considered for each network security control device, b) The CKMS design shall specify which of the mitigation techniques specified in this section are to be employed for each envisioned compromise scenario, and c) The CKMS design shall specify any additional or alternative mitigation techniques that are to be employed.	**Modify**	Modify					
FR:6.117	The CKMS design shall specify any personnel compromise detection features that are provided for each supported role.	Same	Same					
FR:6.118	The CKMS design shall specify any personnel compromise minimization features that are provided for each supported role.	Same	Same					
FR:6.119	The CKMS design shall specify the CKMS compromise recovery capabilities that are provided for each supported role.	Same	Same					
FR:6.120	The CKMS design shall specify how all CKMS components and devices are protected from unauthorized physical access.	**Modify**	Modify					
FR:6.121	The CKMS design shall specify how the CKMS detects unauthorized physical access.	**Modify**	Same					
FR:6.122	The CKMS design shall specify how the CKMS recovers from unauthorized physical access to components and devices other than cryptographic modules.	**Modify**	Same					
FR:6.123	The CKMS design shall specify the entities that are automatically notified if a physical security breach of any CKMS component or device is detected by the CKMS.	**Modify**	Same					
FR:6.124	The CKMS design shall specify how breached areas can be re-established to a secure state.	**Modify**	Same					
	Interoperability and Transitioning				8	0	0	8
FR:7.1	The CKMS design shall specify how interoperability requirements across device interfaces are to be satisfied.	Same	Same					
FR:7.2	The CKMS design shall specify the standards, protocols, interfaces, supporting services, commands and data formats required to interoperate with the applications it is intended to support.	Same	Same					
FR:7.3	The CKMS design shall specify the standards, protocols, interfaces, supporting services, commands and data formats required to interoperate with other CKMS for which interoperability is intended.	Same	Same					
FR:7.4	The CKMS design shall specify all external interfaces to applications and other CKMS.	Same	Same					

NIST Req #	NIST 800-130 Requirement Text	Evernym Classification	Digital Bazaar Classification		Same	Modified	N/A	Total
FR:7.5	The CKMS design shall specify all provisions for transitions to new, interoperable, peer devices.	Same	Same					
FR:7.6	The CKMS design shall specify any provisions provided for upgrading or replacing its cryptographic algorithms.	Same	Same					
FR:7.7	The CKMS design shall specify how interoperability will be supported during cryptographic algorithm transition periods.	Same	Same					
FR:7.8	The CKMS design shall specify its protocols for negotiating the use of cryptographic algorithms and key lengths.	Same	Same					
	Security Controls				6	13	0	19
FR:8.1	The CKMS design shall specify each of its CKMS devices and their intended purposes.	**Modify**	Modify					
FR:8.2	The CKMS design shall specify the physical security controls for protecting each device containing CKMS components.	**Modify**	Modify					
FR:8.3	The CKMS design shall specify all secure operating system requirements (including any required operating system configurations) for each CKMS device.	**Modify**	Modify					
FR:8.4	The CKMS design shall specify which of the following hardening features are enforced by the CKMS: a) Removing all non-essential software programs and utilities from the computer; b) Using the principle of least privilege to control access to sensitive system features and applications; c) Using the principle of least privilege to control access to sensitive system and application files and data; d) Limiting user accounts to those needed for legitimate operations, i.e., disabling or deleting the accounts that are no longer required; e) Running the applications with the principle of least privilege; f) Replacing all default passwords and keys with strong passwords and randomly generated keys, respectively; g) Disabling or removing network services that are not required for the operation of the system; h) Disabling or removing all other services that are not required for the operation of the system; i) Disabling removable media, or disabling automatic run features on removable media and enabling automatic malware checks upon media introduction; j) Disabling network ports that are not required for the system operation; k) Enabling optional security features as appropriate; and l) Selecting other configuration options that are secure.	**Modify**	Same					
FR:8.5:	The CKMS design shall specify the BIOS protection features that ensure the proper instantiation of the operating system.	**Modify**	Same					
FR:8.6	The CKMS design shall specify the security controls required for each CKMS device.	**Modify**	Same					
FR:8.7	The CKMS design shall specify the device/CKMS secure configuration requirements and guidelines that the hardening is based upon.	**Modify**	Same					
FR:8.8	The CKMS design shall specify the following malware protection capabilities for CKMS devices: a) Anti-virus protection software, including the specified time periods and events that trigger anti-virus scans, software update, and virus signature database updates; b) Anti-spyware protection software, including the specified time periods and events that trigger anti-spyware scans, software update, and virus signature updates; and c) Rootkit detection and protection software, including the specified time periods and events that trigger rootkit detection, software update, and signature updates.	**Modify**	Same					
FR:8.9	The CKMS design shall specify the following software integrity check information for operating system and CKMS application software: a) If software integrity is verified upon installation, indicate how the verification is performed; and b) If software integrity is verified periodically, indicate how often the verification is performed.	**Modify**	Same					
FR:8.10	The CKMS design shall specify the auditable events supported and indicate whether each event is fixed or selectable.	Same	Same					
FR:8.11	For each selectable, auditable event, the CKMS design shall specify the role(s) that has the capability to select the event.	Same	Same					
FR:8.12	For each auditable event, the CKMS design shall specify the data to be recorded.	Same	Same					
FR:8.13	The CKMS design shall specify what automated tools are provided to assess the correct operation and security of the CKMS.	**Modify**	Same					
FR:8.14	The CKMS design shall specify system-monitoring requirements for sensitive system files to detect and/or prevent their modification or any modification to their security attributes, such as their access control lists.	**Modify**	Same					
FR:8.15	The CKMS design shall specify the boundary protection mechanisms employed by the CKMS.	**Modify**	Same					
FR:8.16	The CKMS design shall specify: a) The types of firewalls used and the protocols permitted through the firewalls, including the source and destination for each type of protocol; and b) The types of intrusion detection and prevention systems used, including their logging and security breach reaction capabilities.	N/A	Same					
FR:8.17	The CKMS design shall specify the methods used to protect the CKMS devices against denial of service.	Same	Same					
FR:8.18	The CKMS design shall specify how each method used protects against the denial of service.	Same	Same					
FR:8.19	The CKMS design shall identify the cryptographic modules that it uses and their respective security policies, including: a) The embodiment of each module (software, firmware, hardware, or hybrid), b) The mechanisms used to protect the integrity of each module, c) The physical and logical mechanisms used to protect each module's cryptographic keys, and d) The third-party testing and validation that was performed on each module (including the security functions) and the protective measures employed by each module.	**Modify**	Same					
	Testing and System Assurances				9	8	0	17
FR:9.1	A CKMS design shall specify the non-proprietary vendor testing that was performed on the system and passed.	**Modify**	Same					
FR:9.2	The CKMS design shall specify all third-party testing programs that have been passed to date by the CKMS or its devices.	**Modify**	Same					
FR:9.3	If a CKMS claims interoperability with another system, then the CKMS design shall specify the tests that have been performed and passed that verify the claim.	Same	Same					
FR:9.4	If a CKMS claims interoperability with another system, then the CKMS design shall specify any configuration settings that are required for interoperability.	Same	Same					
FR:9.5	The CKMS design shall specify all self-tests created and implemented by the designer and the corresponding CKMS functions whose correct operation they verify.	Same	Same					
FR:9.6	The CKMS design shall specify all scalability analysis and testing performed on the system to date.	Same	Same					
FR:9.7	The CKMS design shall specify the functional and security testing that was performed on the system and the results of the tests.	Same	Same					
FR:9.8	The CKMS design shall specify the environmental conditions in which the CKMS is designed to be used.	**Modify**	Same					

NIST Req #	NIST 800-130 Requirement Text	Evernym Classification	Digital Bazaar Classification		Same	Modified	N/A	Total
FR:9.9	The CKMS design shall specify the results of environmental testing that was performed on the CKMS devices, including the results of all tests stressing the devices beyond the conditions for which they were designed.	**Modify**	Same					
FR:9.10	The CKMS design shall specify: a) The devices (including their source code, documentation, build scripts, executable code, firmware, hardware, documentation, and test code) to be kept under configuration control. b) The protection requirements (e.g., formal authorizations and proper record keeping) to ensure that only authorized changes are made to the components and devices under configuration control.	**Modify**	Same					
FR:9.11	The CKMS design shall specify secure delivery requirements for the products used in the CKMS, including: a) Protection requirements to ensure that the product has not been tampered with during the delivery process or that tampering is detected, b) Protection requirements to ensure that the product has not been replaced during the delivery process or that replacement is detected, c) Protection requirements to ensure that an unrequested delivery is detected, and d) Protection requirements to ensure that the product delivery is not suppressed or delayed and that suppression or delay is detected.	**Modify**	Same					
FR:9.12	The CKMS design shall specify the security requirements for the development and maintenance environments of the CKMS, including: a) Physical security requirements, b) Personnel security requirements, such as clearances and background checks for developers, testers, and maintainers, c) Procedural security, such as multi-person control and separation of duties, d) Computer security controls to protect the development and maintenance environment and to provide access control to permit authorized user access, e) Network security controls to protect the development and maintenance environment from hacking attempts, f) Cryptographic security control to protect the integrity of software and its control data under development, and g) The means used to ensure that the tools (e.g., editors, compiler, software linkers, loaders, etc.) are trustworthy and are not sources of malware.	**Modify**	Same					
FR:9.13	The CKMS design shall specify the CKMS capabilities for detecting system flaws, including: a) Known-answer tests, b) Error detection codes, c) Anomaly diagnostics, and d) Functional Testing.	Same	Same					
FR:9.14	The CKMS design shall specify the CKMS capability for reporting flaws, including: the capability to produce status report messages with confidentiality, integrity and source authentication protections, and to detect unauthorized delays.	Same	Same					
FR:9.15	The CKMS design shall specify the CKMS capability for analyzing flaws and creating/obtaining fixes for likely or commonly known flaws.	Same	Same					
FR:9.16	The CKMS design shall specify its capability to transmit fixes with confidentiality, integrity and source authentication protections and to detect unauthorized delays.	Same	Same					
FR:9.17	The CKMS design shall specify its capability for implementing fixes in a timely manner.	**Modify**	Modify					
	Disaster Recovery				6	3	3	12
FR:10.1	The CKMS design shall specify the required environmental, fire, and physical access control protection mechanisms and procedures for recovery from damage to the primary and all backup facilities.	N/A	N/A					
FR:10.2	The CKMS design shall specify the minimum as well as recommended electrical, water, sanitary, heating, cooling, and air filtering requirements for the primary and all backup facilities.	N/A	N/A					
FR:10.3	The CKMS design shall specify the communications and computation redundancy present in the design and required to be available during operation in order to assure continued operation of services commensurate with the anticipated needs of users, enterprises, and CKMS applications.	N/A	N/A					
FR:10.4	The CKMS design shall specify the strategy for backup and recovery from failures of hardware components and devices.	Same	Same					
FR:10.5	The CKMS design shall specify all techniques provided by the CKMS to verify the correctness of the system software.	Same	Same					
FR:10.6	The CKMS design shall specify all techniques provided by the CKMS to detect alterations or garbles to the software once it is loaded into memory.	Same	Same					
FR:10.7	The CKMS design shall specify the strategy for backup and recovery from a major software failure.	Same	Same					
FR:10.8	The CKMS design shall specify what self-tests are used by each cryptographic module to detect errors and verify the integrity of the module.	**Modify**	Same					
FR:10.9	The CKMS design shall specify how each cryptographic module responds to detected errors.	**Modify**	Same					
FR:10.10	The CKMS design shall specify its strategy for the repair or replacement of failed cryptographic modules.	**Modify**	Same					
FR:10.11	The CKMS design shall specify its procedures for backing-up and archiving cryptographic keys and their metadata.	Same	Same					
FR:10.12	The CKMS design shall specify its procedures for restoring or replacing corrupted keys and metadata that have been stored or transmitted.	Same	Same					
	Security Assessment				15	1	0	16
FR:11.1	The CKMS design shall specify the necessary assurance activities to be undertaken prior to or in conjunction with a full CKMS security assessment.	Same	Same					
FR:11.2	The CKMS design shall specify the circumstances under which a full security assessment is repeated.	Same	Same					
FR:11.3	The CKMS design shall specify all validation programs under which any of the CKMS devices have been validated.	Same	Same					
FR:11.4	The CKMS design shall specify all validation certificate numbers for its validated devices.	**Modify**	Modify					
FR:11.5	The CKMS design shall specify whether an architectural review is required as part of the full security assessment.	Same	Same					
FR:11.6	If an architectural review is required, then the CKMS design shall specify the skill set required by the architectural review team.	Same	Same					
FR:11.7	The CKMS design shall specify all required functional and security testing of the CKMS.	Same	Same					
FR:11.8	The CKMS design shall report the results of all functional and security tests performed to date.	Same	Same					
FR:11.9	The CKMS design shall specify the results of any completed penetration testing performed to date.	Same	Same					
FR:11.10	The CKMS design shall specify the periodicity of security reviews.	Same	Same					
FR:11.11	The CKMS design shall specify the scope of the security review in terms of the CKMS devices.	Same	Same					
FR:11.12	The CKMS design shall specify the scope of the periodic security review in terms of the activities undertaken for each CKMS device under review.	Same	Same					
FR:11.13	The CKMS design shall specify the functional and security testing to be performed as part of the periodic security review.	Same	Same					

NIST Req #	NIST 800-130 Requirement Text	Evernym Classification	Digital Bazaar Classification		Same	Modified	N/A	Total
FR:11.14	The CKMS design shall specify the circumstances under which an incremental security assessment should be conducted.	Same	Same					
FR:11.15	The CKMS design shall specify the scope of incremental security assessments.	Same	Same					
FR:11.16	The CKMS design shall list the hardening activities required to be performed in order to maintain its security.	Same	Same					
	Technological Challenges				6	2	0	8
FR:12.1	The CKMS design shall specify the expected security lifetime of each cryptographic algorithm implemented in the system.	Same	Same					
FR:12.2	The CKMS design shall specify which sub-functions (e.g., the hash sub- function of HMAC) of the cryptographic algorithms can be upgraded or replaced with similar, but cryptographically improved, sub-functions without negatively affecting the CKMS operation.	Same	Same					
FR:12.3	The CKMS design shall specify which key establishment protocols are implemented by the system.	Same	Same					
FR:12.4	The CKMS design shall specify the expected security lifetime of each key establishment protocol implemented in the system in terms of the expected security lifetimes of the cryptographic algorithms employed.	Same	Same					
FR:12.5	The CKMS design shall specify the extent to which external access to CKMS devices is permitted.	**Modify**	Modify					
FR:12.6	The CKMS design shall specify how all allowed external accesses to CKMS devices is controlled.	**Modify**	Modify					
FR:12.7	The CKMS design shall specify the features employed to resist or mitigate the consequences of the development of new technologies, such as a quantum computing attack upon the CKMS cryptographic algorithms.	Same	Same					
FR:12.8	The CKMS design shall specify the currently known consequences of a quantum computing attack upon the CKMS cryptography.	Same	Same					
								258
	ANALYSIS							
			Percentage					
	Same	163	63%					
	Modifed	85	33%					
	N/A	10	4%					
	TOTAL	258