

Comment Number	Category	Page	Sub clause	Line	Comment	Proposed Change	Resolution Status	Resolution Detail	Discuss?
1	Editorial	2	3.1	11	The term "Policy" isn't defined in Section 3.1. This seems like a fundamental concept, and we might want to consider defining it.	Add section 3.1.37 to include Policy in Draft	Completed	Added 3.1.37 Policy : A rule that defines one or more requirements for how a key or group of keys are generated, used, distributed, retained, audited and/or stored.	No
2	Technical	16	4.4.2	21	Do we want to include the ASN.1 definition of a SO_GUID in Section 4.4.2? Many people have never used ABNF and don't understand it, and as long as we don't specify a particular encoding rule (BER, DER, etc.), the ASN.1 definition really does the same thing.	Decide as a group to use ASN.1 and/or ABNF for defining name spaces and other objects. We have a preliminary ASN.1 version provided by Luther Martin that can be shown in a side by side comparison			Yes
3	Technical	27	6.1	12	To guarantee interoperability, we probably need to specify more detail for the HTTP over SSL in Section 6.1. Requiring compliance with RFC 2818 might be a good way to do this.	Include appropriate RFC's used in section 2 and refer to them accordingly in Section 6.1			Yes
4	Editorial	27	6.1	12	We also might want to replace references to SSL with references to TLS. Due to arcane crypto details, you can't use SSL and be FIPS 140-2 compliant, but using TLS is fine.	Modify to a TLS. Suggest specifying which version of TLS to use (1.0 or 1.2) and including specification reference as part of section 2.0 normative references.	Partial	Modified in Draft 3 from "over an SSL encrypted connection" to "over a TLS encrypted connection"	No
5	Editorial	2	3.1	11	General suggestion for the document: There are a number of definitions that are phrases. Occasionally subsets of these phrases appear in the document as descriptive text. Consider highlighting (say with italics) whenever a definition is used so that the other instances are not confused as possibly being a typo.	Use dynamic links where phrases are used to definitions within electronic document.			No
6	Editorial	3	3.1.9	3	Definition is confusing, can it be improved? Should "data attributes" be "data set attributes" as is defined below?	Revise definition based on section 4.2 and 4.3 uses.	Completed	Replaced with 3.1.12 Data set : A collection of data independent of structure, media or transport that are to be encrypted using a common key.	No
7	Editorial	3	3.1.10	5	What is a user set?	Replace 3.1.10 definition based on definition of 3.1.9 and section 4.3 examples	Completed	Replaced with 3.1.13 Data set attribute : A specific attribute such as file path, tape volume id, server IP, a range of disk blocks or database column identifier that can be used to define a policy for how one or more data sets are to be protected.	No
8	Editorial	6	4.1	5	What does see 5 refer to? Page 5, Section 5, Reference 5?	Request information from Subhash & Ravi on specifics			
9	Editorial	7	4.3.1	29	The title should be kept with the figure	Changes with each draft. Will ensure they stay together from this point forward.	Completed	Repaginate document as last edit function of Draft 3.	No
10	Editorial	8	4.3.1	1	Shouldn't this be "data set attributes" based on the preceding text (Page 7, Line 27).	Section revised by Architecture Adhoc information	Completed	Revised by replacement in Draft 3 using Architecture Adhoc proposal.	No
11	Editorial	8	4.3.2	6	Formatting of these paragraphs should coincide with following paragraphs.	Section revised by Architecture Adhoc information	Completed	Revised by replacement in Draft 3 using Architecture Adhoc proposal.	No

Comment Number	Category	Page	Sub clause	Line	Comment	Proposed Change	Resolution Status	Resolution Detail	Discuss?
12	Editorial	8	4.3.2	25	It is sort of implied, but I think it would be good to explicitly confirm in the text that an Expired key can be used for reading data (i.e. decryption with this key is allowed).	Section revised by Architecture Adhoc information	Completed	Revised by replacement in Draft 3 using Architecture Adhoc proposal.	No
13	Editorial	9	4.3.2	4	Don't have this figure sit between the section heading and its items.	Section revised by Architecture Adhoc information	Completed	Revised by replacement in Draft 3 using Architecture Adhoc proposal.	No
14	Editorial	9	4.3.3	10	I think this should be "data set bindings" to maintain conformance with the definitions and the subsequent section title.	Section revised by Architecture Adhoc information	Completed	Revised by replacement in Draft 3 using Architecture Adhoc proposal.	No
15	Editorial	11	4.3.3.3	36 & 37	It is not clear what the "response" is or what it implies.	Section revised by Architecture Adhoc information	Completed	Revised by replacement in Draft 3 using Architecture Adhoc proposal.	No
16	Editorial	12	4.3.3.3	1	It is not clear what the "response" is or what it implies.	Section revised by Architecture Adhoc information	Completed	Revised by replacement in Draft 3 using Architecture Adhoc proposal.	No
17	Editorial	12	4.3.3.3	8	There should be no newline here.	Section revised by Architecture Adhoc information	Completed	Revised by replacement in Draft 3 using Architecture Adhoc proposal.	No
18	Editorial	12	4.3.3.3	9	Where is the example?	Section revised by Architecture Adhoc information	Completed	Revised by replacement in Draft 3 using Architecture Adhoc proposal.	No
19	Editorial	12	4.3.3.4	20	Delete the word the	Section revised by Architecture Adhoc information	Completed	Revised by replacement in Draft 3 using Architecture Adhoc proposal.	No
20	Editorial	12	4.3.3.4	22	will be kept forever	Section revised by Architecture Adhoc information	Completed	Revised by replacement in Draft 3 using Architecture Adhoc proposal.	No
21	Editorial	12	4.3.3.4	29	Clarify the term "time triple"	Section revised by Architecture Adhoc information	Completed	Revised by replacement in Draft 3 using Architecture Adhoc proposal.	No
22	Editorial	13	4.3.3.5	4	Not clear what "This" is referring to. Be more specific. Should "which" be "with" - as is sentence phrasing is awkward.	Section revised by Architecture Adhoc information	Completed	Revised by replacement in Draft 3 using Architecture Adhoc proposal.	No
23	Editorial	13	4.3.4	6	Aren't there more valid key types that should appear here, or is this merely intended to provide examples and not an exhaustive list of possibilities?	Section revised by Architecture Adhoc information	Completed	Revised by replacement in Draft 3 using Architecture Adhoc proposal.	No
24	Editorial	13	4.3.4.1	22	limited	Section revised by Architecture Adhoc information	Completed	Revised by replacement in Draft 3 using Architecture Adhoc proposal.	No
25	Editorial	15	4.4.1	23	Need to fix this reference	Changed to Annex E (Informative)	Completed	Removed Section 4.4.2 reference and replaced with Annex E link & reference.	No
26	Editorial	20	4.4.3	20	Bullet should align with the previous one.	Aligned	Completed	Aligned bullets with Bullet a	No
27	Editorial	22	4.4.4	1	Bullet should start with "a"	Corrected	Completed	Restarted numbering at a)	No
28	Technical	22	4.4.5	12	What does this mean? 1 to 8 digits from the set [0-9]? Any number of digits from the set [1-8]?	Need input from OASIS EKMI group			
29	Editorial	22	4.4.5	18	Isn't this one invalid, because it is too long? Depending on the meaning of DIGIT 1*8, the preceding example may be invalid as well.	Need input from OASIS EKMI group			
30	Editorial	23	5.3.1	23	Summary is bold in subsequent sections	Corrected	Completed	Made font bold	

Comment Number	Category	Page	Sub clause	Line	Comment	Proposed Change	Resolution Status	Resolution Detail	Discuss?
31	Editorial	23	5.3.3	31	Is there expected to be any coordination of time between KMS's and clients? If not, how can audit logs be related?	Need to add verbiage that field for time stamp from both KM Client and KM Server are stored with each log entry generated by CU or KM Client. This will alleviate the issue of differences in time.			Yes
32	Editorial	24	5.5.1	24	that was selected	corrected	Completed	added was	
33	Technical	25	5.5.1	5	Suppose we are talking about tape operations here. Whenever a tape is experiencing a write operation from the beginning, then a new key should be generated. One would expect that this request would be used. But if the tape was previously encrypted, this note tends to imply that the client must generate the key. Perhaps more clarification is required.	Specify that overwriting of media requires a new key for that media.			Yes
34	Technical	25	5.5.3	23	Should a KMS really be returning "all matching keys" as a result of a query? I would expect that it might return information about keys that match, but not the keys themselves. Ultimately I would expect that a client would be sent a single key that it is authorized to use.	Specify specific use cases where more than one key can be returned otherwise we need to discuss this.			Yes
35	Technical	25	5.5.4	26	I know that existing implementations permit clients to generate and store keys, BUT if a KMS is to provide quality assurance of a key and long term availability to it, then I think that ALL keys must be generated by the KMS. Otherwise, clients will do as we do now, and that is to assume that the KMS cannot be trusted and only store wrapped keys there.	There are specific cases where end points can generate higher quality keys than the KMS. In these cases we need the option to support both. While most keys will be generated in the KMS cloud, there will be some that have FIPS or other reasons to generate their own.			Yes
36	Editorial	31	6.1.2	2	containing what?	Need additional input from Subhash or Ravi.			

Comment Number	Category	Page	Sub clause	Line	Comment	Proposed Change	Resolution Status	Resolution Detail	Discuss?
37	Technical	49	B.2	18	<p>Backup applications require the creation of very elaborate policy rules.</p> <p>For example, organizations typically perform daily, weekly, monthly and annual backups each with their own specific requirements for retention policies.</p> <p>But whether a particular backup will require the attributes associated with daily, weekly, monthly or annual is actually a function of when the backup is created.</p> <p>Most KMS systems that I have seen to date, do not allow retention policy selection based on qualifying the current date.</p>	<p>This will need to be considered when media (such as LTO4) or application based encryption use more than one key per media. Maintaining the appropriate time stamps should allow this for at least the backup applications.</p> <p>LTO4 drives may have issues if they can not find all the keys for a given media. Need clarification on this from LTO4 vendors.</p>			Yes
38	Editorial	9	4.1	9	<p>The intro section regarding advantages of centralizing key management needs to be clarified. I think the three listed (eg. centralized policy mgmt, etc) needs to be expanded as some readers may not see them as being advantages. Also, it is perhaps worthwhile to mention that any security functionality that is centralized has an increased risk of being a sole target of attack.</p>				
39	Editorial	11		6	<p>Data-at-rest protection. It would be useful to stay with one phrase or terminology. I would suggest "data-at-rest" protection, since this spec does not cover data-in-transit protection. This would then be consistent with Figure 1 and the definition of "Storage Medium" (p11, line 6).</p>				
40	Editorial	12		6	<p>Control Plane (p12, line 6): I think this sentence is missing the KM Server entity. Looking at Figure 2, the control plane covers the movement of keys and keying-material anywhere from the (a) KM Server to KM Client, (b) KM Client to Crypto-Unit (inside KM Client) and (c) KM-Server direct to Crypto-unit.</p> <p>[ps. unless I'm simply not understanding the definition].</p>				

Comment Number	Category	Page	Sub clause	Line	Comment	Proposed Change	Resolution Status	Resolution Detail	Discuss?
41	Technical	15	4.4.1.1	5	Key State Definitions (4.4.1.1) on p15, line 5. The definition says that a key in Pre-Activation state can *only exist* in the KM Server. However, the next line then says that the key can be distributed to a KM client (which means that the key is no longer solely in the KM Server). Perhaps this definition needs clarification.				
42	Editorial	16 18		21 18	There needs to be some adjustment or clarification between p16/line 21 and p18/line 18. Reading these two paragraphs, I got confused as (a) who is generating the key and (b) who is delivering to whom.				