20030223

OK, in collecting BPsec information to try to get a resolution to Tomaso I think we're not there yet.

I think the largest outstanding item is Annex D where we tried to profile the IETF default security contexts. I think that if we profile in changes to e.g. the key lengths as Mehmet suggests, that would define a NEW security context that we'd need to register w/ IANA. So I think our options are:

1. Remove annex D and simply reference the IETF default security contexts; define CCSDS-specific security contexts in TBD new documents.

2. Proceed with a profile as in annex D and use that to register NEW security contexts with IANA (essentially the existing IANA ones with our profile changes).

3. Work to define new CCSDS security contexts, replace Annex D with those, and use it to register the new contexts w/ IANA.

I KNOW we talked about this, but I'm having difficulty getting at my older notes at the moment. I THINK we opted for option 1.

And we need to go over Annex A (PICS).

Also, does anybody (APL?) have the original art for the figures in the book? If not we'll have to recreate them.

--keith

========

Proposal:

- Option 1 above: Make Annex D point to 9173 as-is with a note that CCSDS intends to define CCSDS-specific security context(s)
    - Use the RFC9173 security contexts for interoperability testing
    - Implementation of the RFC9173 security contexts by any mission is optional
    - Note: we may require implementation of some TBD CCSDS-specific security contexts

  WG: the above makes sense.

- What to do with E3: “BPSec Application Data Model”
    - Should we leave this to the BPsec ADM definition?

  Remove E3.1
  Leave E3.2 or reformat as a table.

- BPSec or BPsec? (OK, RFC9173 uses BPSec)
-
- Section 3.5 – discussing security context identifier registration
    - Keith suggests that we explicitly state that these will be registered with IANA
- Move annexes F and G to somewhere else.

—----

We need a paragraph or two about how authenticity can be achieved by applying the block types in BPSec together with the security context in which they’re used. [Ed to write]

Section 2.3 add text.

Reference for Key management in section 3.3

Move policy from PICS to green book.