Conclusions

– (Scope) Everything that touches a key is part of the framework
  • Specify appropriate security requirements

– Distinction between framework and profile is not clear

– Narrow down the target readership
  • Designers, operators, security architects
  • Should be possible to turn into actionable vendor requirements

– Needs to answer how to check compliance
  • Gather the “shall” together in an appendix
  • All “shall” need to be measurable

– (Section 11) Need clarity around what audit would look like
  • Should specify that threat modeling is needed
  • Need flexibility in how audit is done, don’t let this creep into compliance

– Section 3 in general
  • Too much motherhood/apple pie in section headers
  • Need better connection to the “shall.”
  • Example: COTS should be build vs buy to make this broader