Framework Breakout Sessions

NIST Key Management Workshop
September 20-21, 2010

Instructions: September 20 (2PM Session)

• Group A will meet in Conference Room A
• Group D will meet in Conference Room D
• Webcast attendees send their comments and ideas to kmwquestions@nist.gov
• Each group selects a note taker and a person who will summarize the group’s discussions and recommendations in the
Instructions: September 20
(3:45PM Session)

• Each group will prepare recommendations for presentation at the plenary session for September 21

Discussion Questions
1-2 General

• Is a Framework useful?
  – What is its most significant value?
  – Would the Framework help you compare two conforming CKMS?

• Is the current Scope about right? If not, what is the proper Scope?

1-2 General

• Is the major components list complete?
  – Subtractions
  – Additions

• Are the requirements at the right level?
  – Too high level
  – Too detailed
  – About right
3. Goals

- Are the goals appropriate?
- Are significant goals missing?
- Is the requirement set appropriate and sufficient?

4. Security Policies

- Is the discussion adequate?
- Is Figure 3 helpful?
- Is the requirement set appropriate and sufficient?
5. Roles and Responsibilities

- Are the example roles adequate?
- Does anything else need to be said about roles and responsibilities?
- Is the requirement set appropriate and sufficient?

6. Cryptographic Keys and Metadata

- Does anything more need to be said about key types?
- Are the key metadata adequately covered?
- Are the sample key states and transitions useful?
- Should a separate diagram be done for
6. Cryptographic Keys and Metadata

• Does anything more need to be said about the key and metadata management functions?
• Are backup, archive, and escrow separate functions?
• Is key establishment adequately handled?
• Any comments on KM function controls?
• Has compromise recovery been adequately addressed?

7. Interoperability and Transition Requirements

• Is the discussion sufficient?
• Is the requirement set appropriate and sufficient?
8. Security Controls

- Is the discussion an adequate summary?
- Is the requirement set appropriate and sufficient?

9. Testing and System Assurance

- Is the spectrum of testing adequately covered?
- Is the requirement set appropriate and sufficient?
10. Disaster Recovery

- Is on-line backup adequately covered?
- Does more need to be said about backup recovery in large networks?
- Is the requirement set appropriate and sufficient?

11. Security Assessment

- Is the security assessment procedure reasonable?
- Should other methods be discussed?
- Should third party architectural review and its relationship to security assessment be further discussed?
- Should automated methods (e.g., SCAP) be
12. Other Considerations

- Are the considerations listed appropriate?
- Do any need to be expanded upon?
- Should other considerations be listed?
- Is the requirement set appropriate and sufficient?

Discussion?