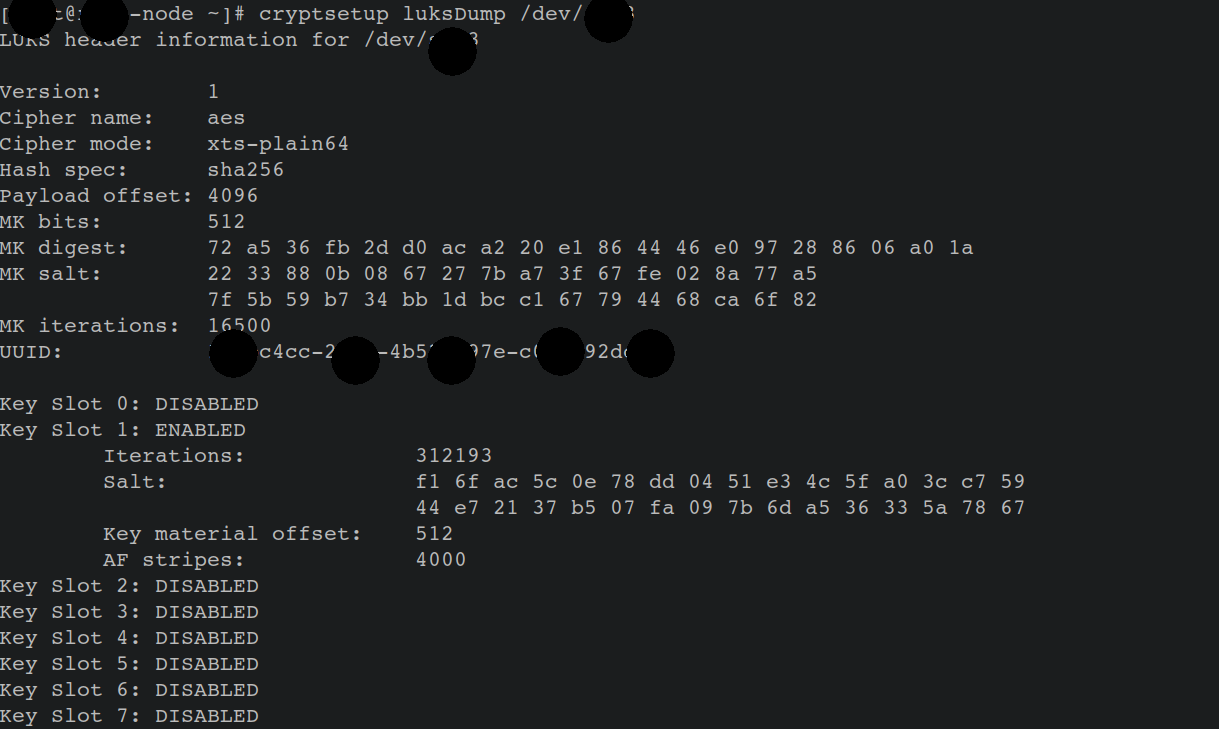
1. Run a status command to confirm the encryption and cipher details.



2. Formal procedures to support split knowledge and dual control encryption key custodians.

Key’s:

section1 and section 2

1. *Dual Control means that no one person alone should be able to manage your encryption keys. Creating, distributing, and defining access controls should require at least two individuals working together to accomplish the task.*
2. *Separation of Duties means that different people should control different aspects of your data protection strategy. This is the old adage “don’t put your eggs in one basket”. The person who creates and manages the keys should not have access to the data they protect. And, the person with access to protected data, should not be able to manage encryption keys.*
3. *Split Knowledge applies to the manual generation of encryption keys, or at any point where encryption keys are available in the clear. More than one person should be required to constitute or re-constitute a key in this situation.*

3. Formal procedures to ensure that key recovery functions exist and only authorized personnel have access to this function.

4. Formal procedures to handle replacement of encryption keys and keying materials in case of known or suspected key compromise, or when an employee with key knowledge separates.

