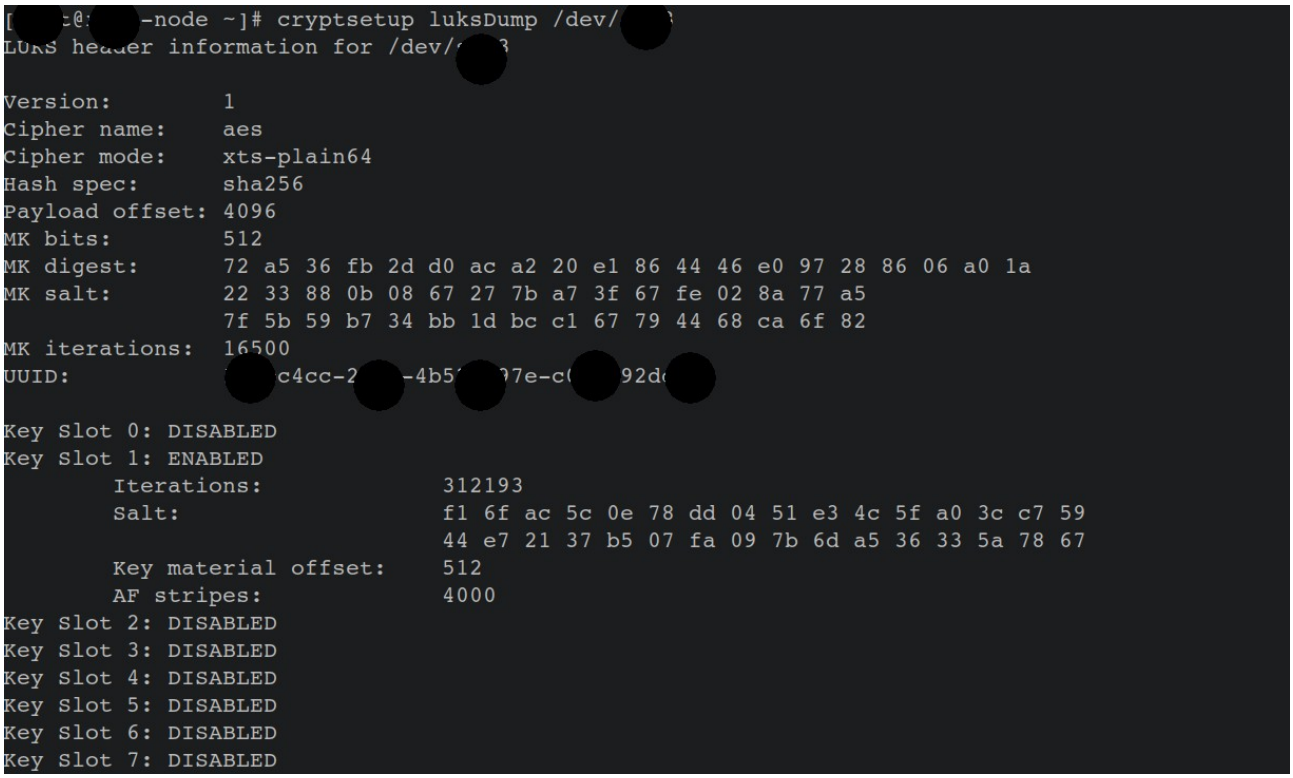
1. Run a status command to confirm the encryption and cipher details.

Here below mentioned the screenshot which is implemented on our side with the status command to confirm the encryption and cipher details.



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

Key's: keys are splitted as section1 and section 2

Split Knowledge applies to the manual generation of encryption keys, or at any point where encryption keys are available in our end based on formal procedures. We split two persons constitute or re-constitute a key in this existing situation.

In our organization for Separation of Duties two peoples are controlling the different aspects of our data protection strategy. 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.

No one person alone should be able to manage the encryption keys. Creating, distributing, and defining access controls should require two individuals working together to accomplish the task.

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

We are using two encryption keys as primary and secondary keys. If we lose our primary key, we have a backup of secondary key to the authorised persons who got approval from our organizations higher authorised authorities.

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.

The resigned persons credentials are removed from the server and all the credentials are given to the replaced authorised person including new encryptions keys and keying materials. However as per our Infosec policy all the confidential keys are changed 90 days once.