

Utilizing Data Encryption and Secrets Management Services

Questions	Notes
Data in flight vs data at rest	<ul style="list-style-type: none">• Data in flight:Data that is moving from one location to another• Data at Rest: data that is inactive or stored for later use
KMS: Key Management service	<ul style="list-style-type: none">• Key generator• store and control keys• Aws manages encryption keys• Automatically enabled for certain services• KMS in the real World:<ul style="list-style-type: none">◦ when you create an encrypted amazon EBS volume, you are able to specify a KMS customer master key
CloudHSM: Hardware security Module	<ul style="list-style-type: none">• used to generate encryption keys• Dedicated hardware for security• generate and manage your own encryption keys• aws does not hace access to your keys
Secrets Manager	<ul style="list-style-type: none">• Allows you to manage and retrieve secrets(passwords or keys)• Rotate, manage and retrieve secrets• encrypt secrets at rest• Integrates with services like rds , Redshift, and DocumentDB• IN the real world:• Retreive database credentials needed for your application code
Things to remmeber for the exam	<ul style="list-style-type: none">• KMS: AWS manages KMS keys• Secret manager: has built-in integration for RDS , Redshift, anad DocumentDB