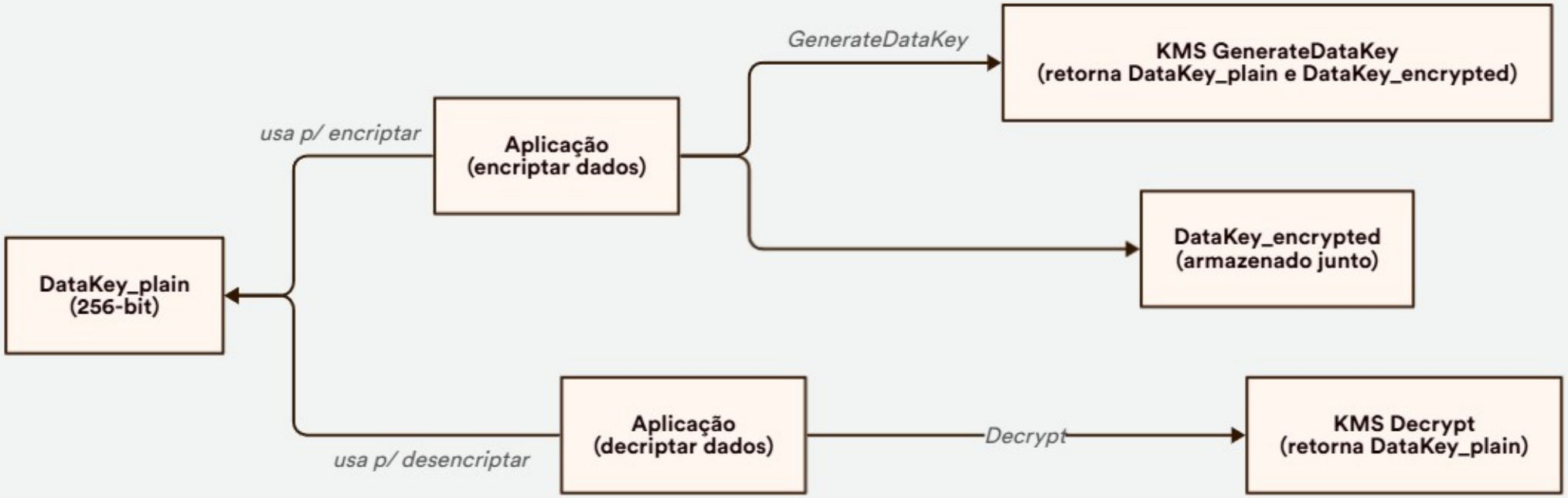
KMS, Parameter Store e Secrets Manager

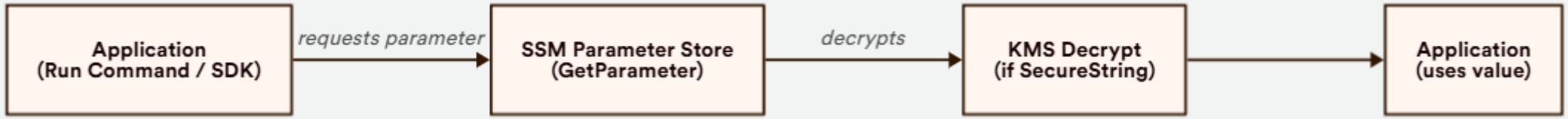
AWS KMS (Key Management Service)

- Serviço para criar, armazenar e gerenciar chaves criptográficas com segurança
- Permite criptografia em repouso para S3, EBS, RDS, etc.
- Suporta chaves gerenciadas pela AWS, pelo cliente (CMK) e por h



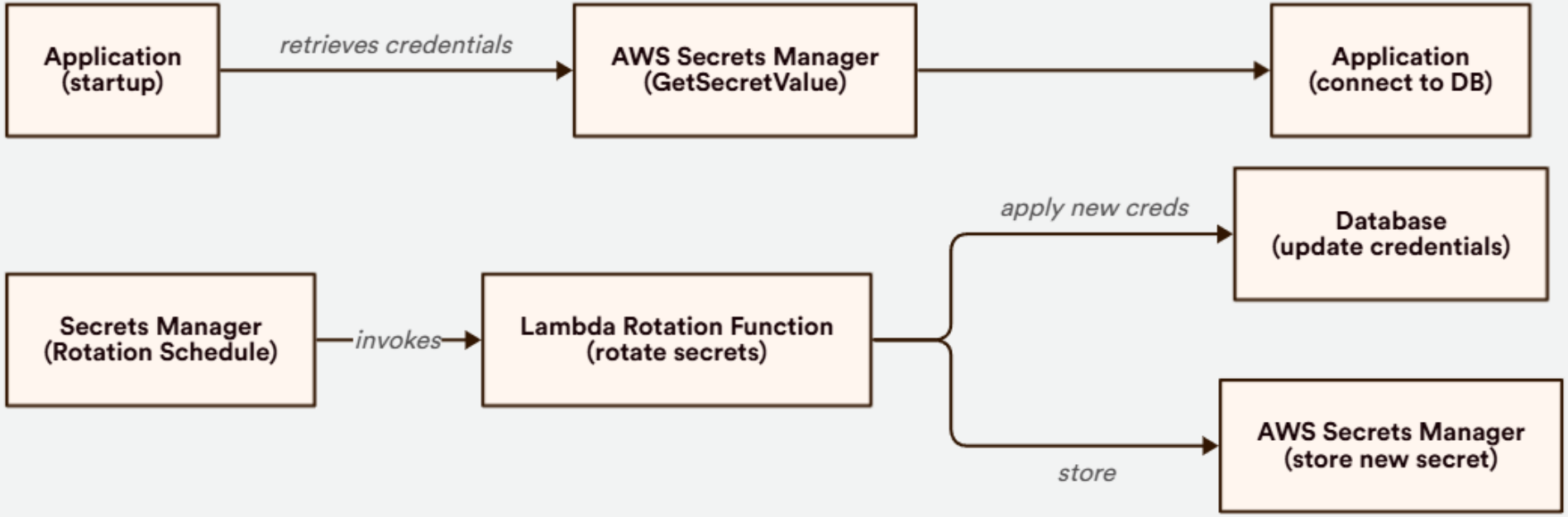
AWS SSM Parameter Store (SSM: Systems Manager)

- Armazena parâmetros de configuração (strings, números, valores secretos)
- Integração nativa com EC2, Lambda e outras aplicações
- Suporta criptografia com KMS e versionamento de parâmetros



AWS Secrets Manager

- Gerencia credenciais e segredos (senhas, tokens, conexões DB, etc.) com rotação automática
- Permite controlar acesso via IAM e auditável com CloudTrail
- Mais robusto que o Parameter Store para segredos sensíveis



Parameter Store vs Secrets Manager

📌 CRITÉRIO	🔑 PARAMETER STORE	🛡️ SECRETS MANAGER	💡 DICA PARA PROVA
Tipo de Dados	Strings, SecureString (criptografado via KMS), parâmetros simples	Segredos: credenciais, tokens, conexões de DB com rotação	**Use Secrets Manager para segredos que precisam de rotação automática.**
Rotação de Segredos	Manual (scripts externos necessários)	Automática via Lambda integrada	**Prova: rotação automática só no Secrets Manager.**
Versionamento	Sim (armazena múltiplas versões de parâmetros)	Sim (histórico de versões de segredo)	**Ambos versionam, mas apenas SM expõe eventos de rotação.**
Custo	Gratuito para parâmetros padrão; cobranças por SecureString e API extra	Tarifa por segredo + chamadas de API	**Parameter Store Standard é gratuito; Secrets Manager não.**
Integração nativa	EC2, Lambda, ECS, SSM Run Command	EC2, Lambda, RDS, Redshift, DocumentDB (rotações built-in)	**Secrets Manager integra com RDS para rotação sem código.**
Casos de Uso	Configurações de aplicação, flags de feature, URLs externas	Credenciais de banco de dados, chaves de API, tokens OAuth	**Parameter Store para configs; SM para segredos críticos.**

Boas Práticas e Dicas de Prova

- KMS é central para criptografia em repouso na AWS – aparece com S3, EBS, RDS, etc.
- Use Parameter Store para configs seguras com acesso simples
- Use Secrets Manager para segredos sensíveis que exigem rotação e auditoria
- A prova pode cobrar diferenças, limites e integração com serviços AWS
- CloudTrail registra uso de KMS e Secrets Manager para rastreabilidade