

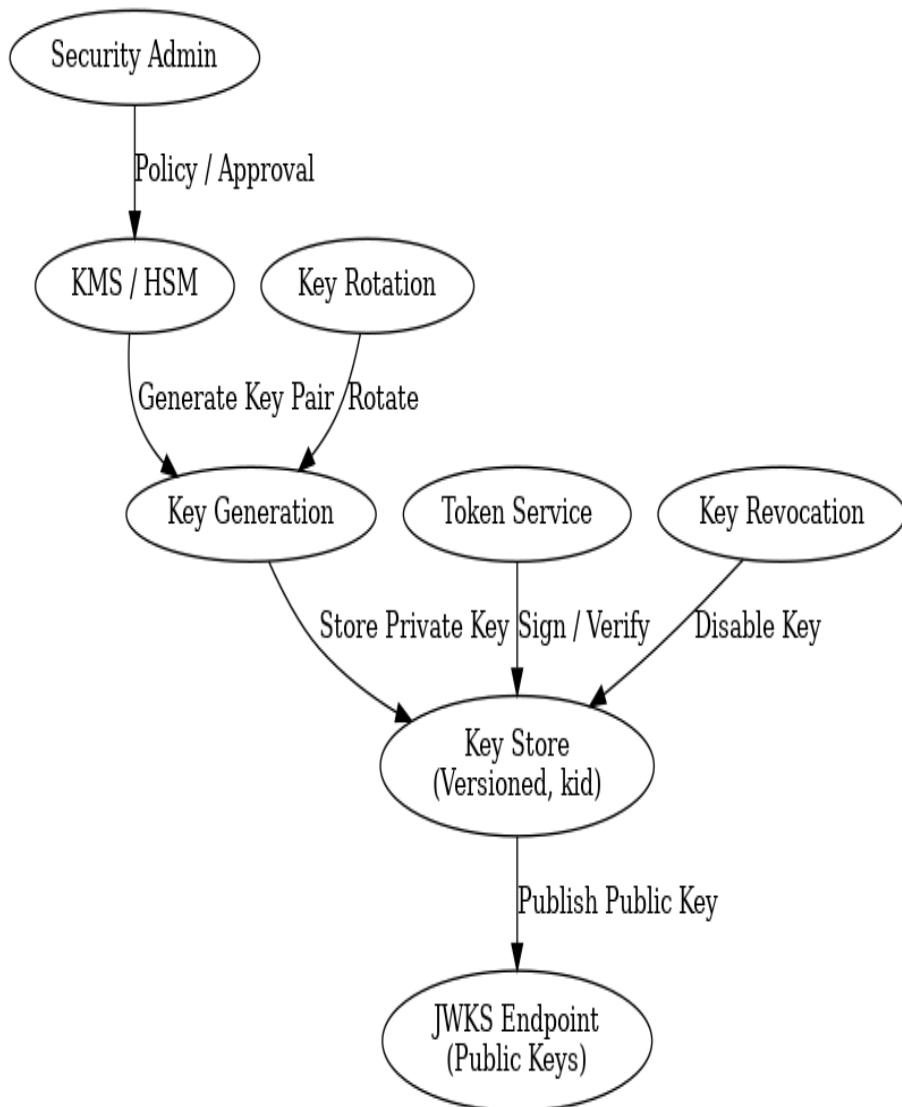
# VianalD – Criptografia e Ciclo de Vida de Chaves (KMS / HSM)

Documento Oficial de Gestão Criptográfica

## 1. Objetivo do Documento

Este documento descreve como o VianalD gera, armazena, rotaciona, publica e revoga chaves criptográficas, garantindo segurança e conformidade.

## 2. Diagrama de Ciclo de Vida de Chaves



## 3. Princípios Criptográficos

- Chaves privadas nunca saem do KMS/HSM - Versionamento por kid - Algoritmos modernos (RSA-2048+, ECDSA, EdDSA) - Assinatura e verificação segregadas

#### **4. Rotação e Revogação**

Rotação é periódica e automática. Revogação é imediata em caso de incidente.

#### **5. Conclusão**

Este modelo garante confidencialidade, integridade e não-repúdio para tokens e comunicações.