

ENCONTRO CCEE

Segurança de Mercado

Painel 3:

Plataforma de Monitoramento Prudencial
Arquitetura da solução

Marcelo Molina

Gerente Executivo de Arquitetura, Desenvolvimento e Operação

16/03/2023

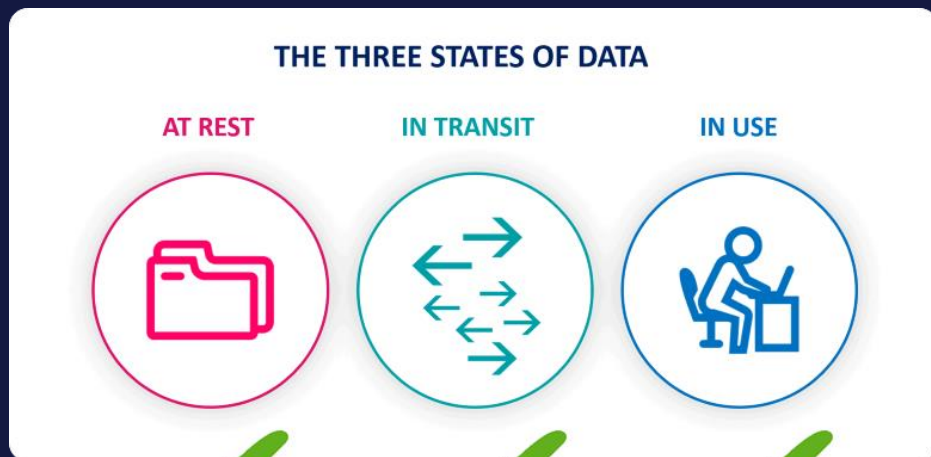


**Infraestrutura computacional
dos demais sistemas CCEE**



- Total segregação de ambientes
- Os dados altamente sensíveis não compartilharão a infraestrutura dos demais sistemas da CCEE
- Mínima quantidade de pessoas com acesso de administração ao ambiente confidencial
- Alta disponibilidade dos sistemas
- Arquitetura *disaster recovery ready*
- Fornecedor escolhido: Amazon Web Services (AWS)

Criptografia completa dos dados



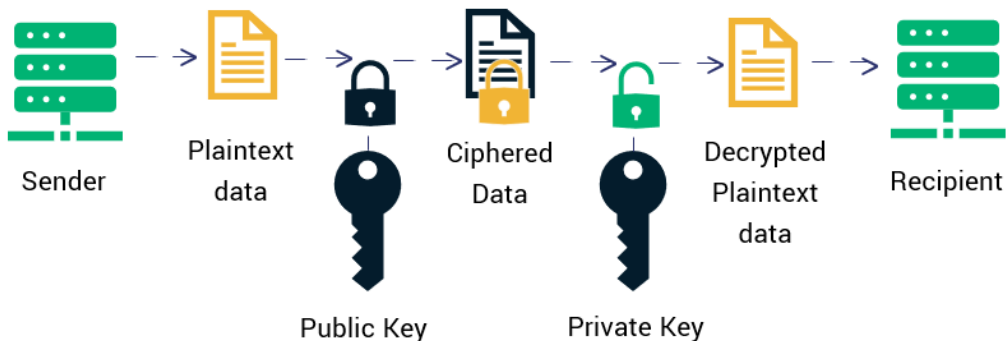
AWS Nitro Enclaves

- Dados permanecem confidenciais mesmo quando em processamento em memória
- Código de software auditável e protegido por assinatura digital contra qualquer violação
- Garantia de segurança a nível de hardware, independente das camadas de sistema operacional ou aplicação
- Adoção da solução AWS Nitro Enclaves



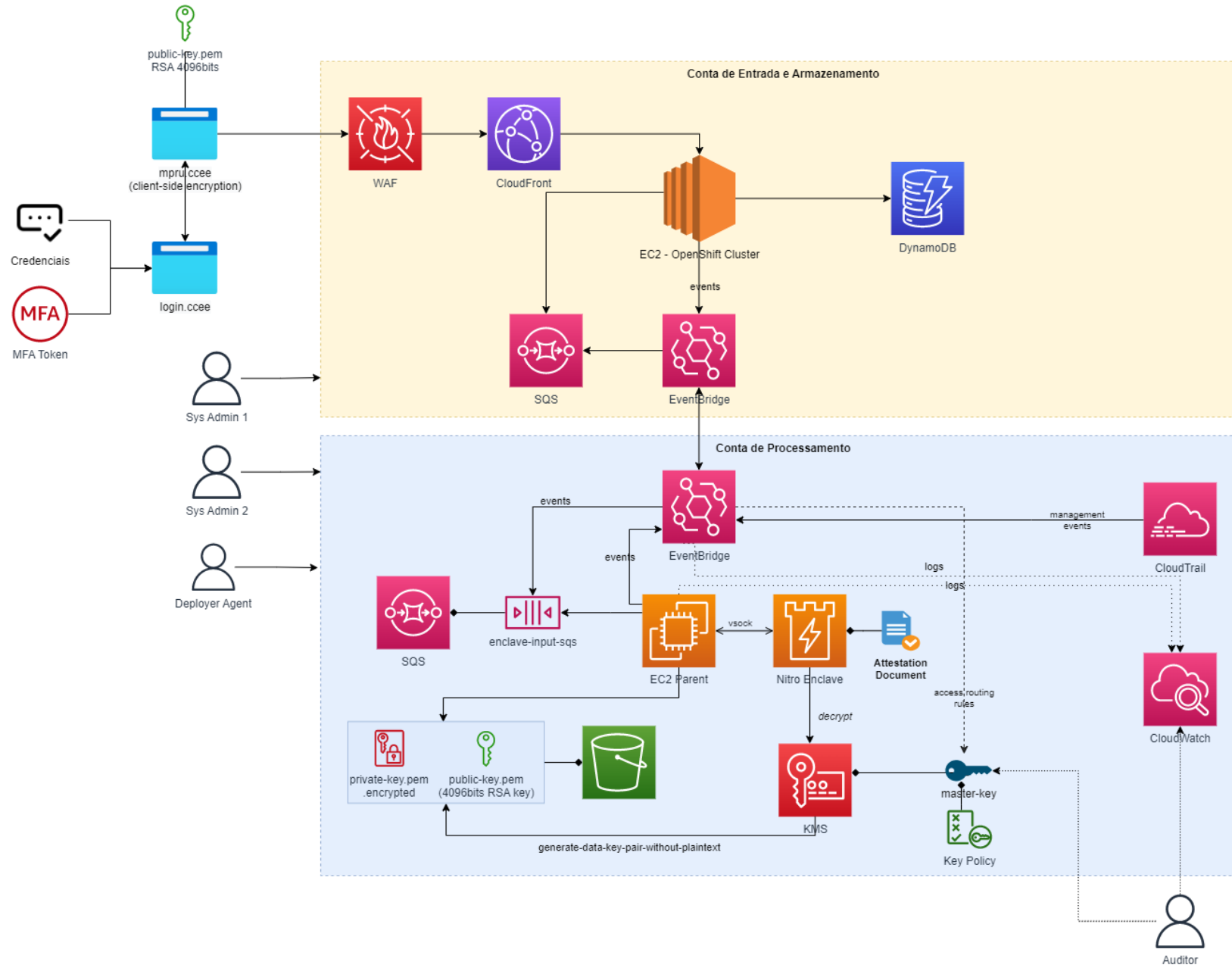
- Dados sensíveis criptografados pelo cliente antes mesmo do envio à CCEE
- Os dados são transmitidos através de canal criptografado de comunicação
- Os dados criptografados são armazenados em banco de dados criptografado
- Processo de criptografia assimétrica RSA, com uso de chave pública e privada
- As chaves são protegidas por uma chave mestra guardada em um Módulo de Segurança em Hardware (HSM)

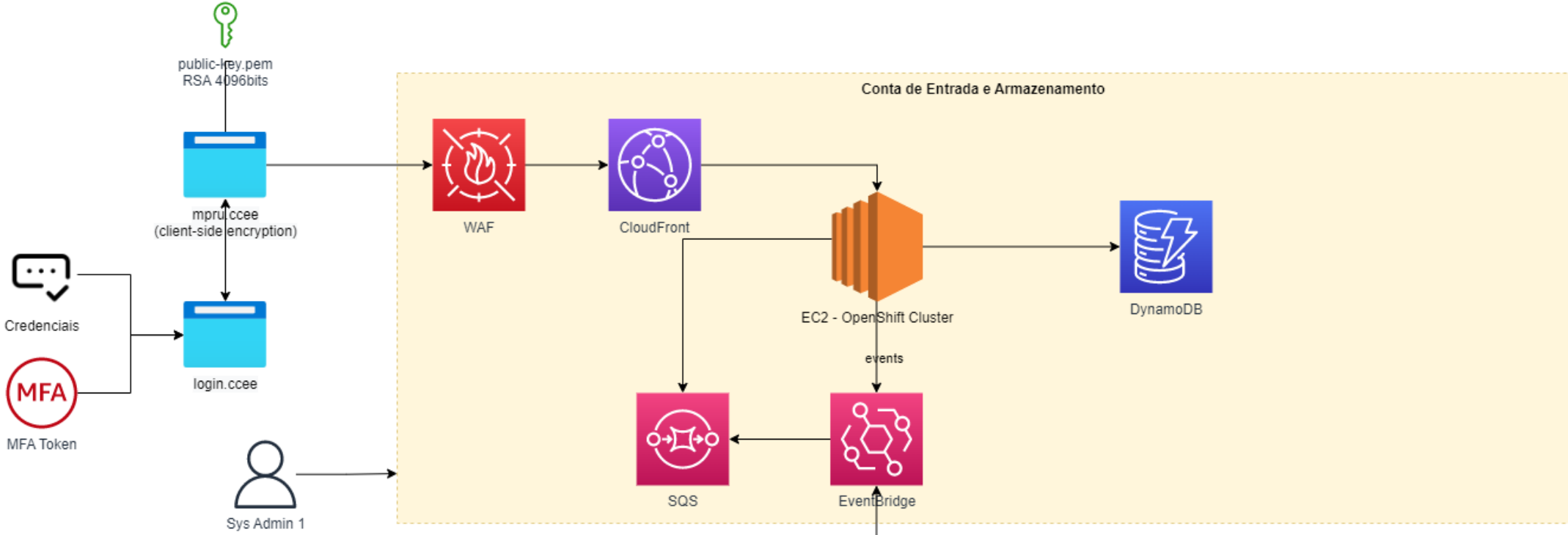
How RSA Encryption Works

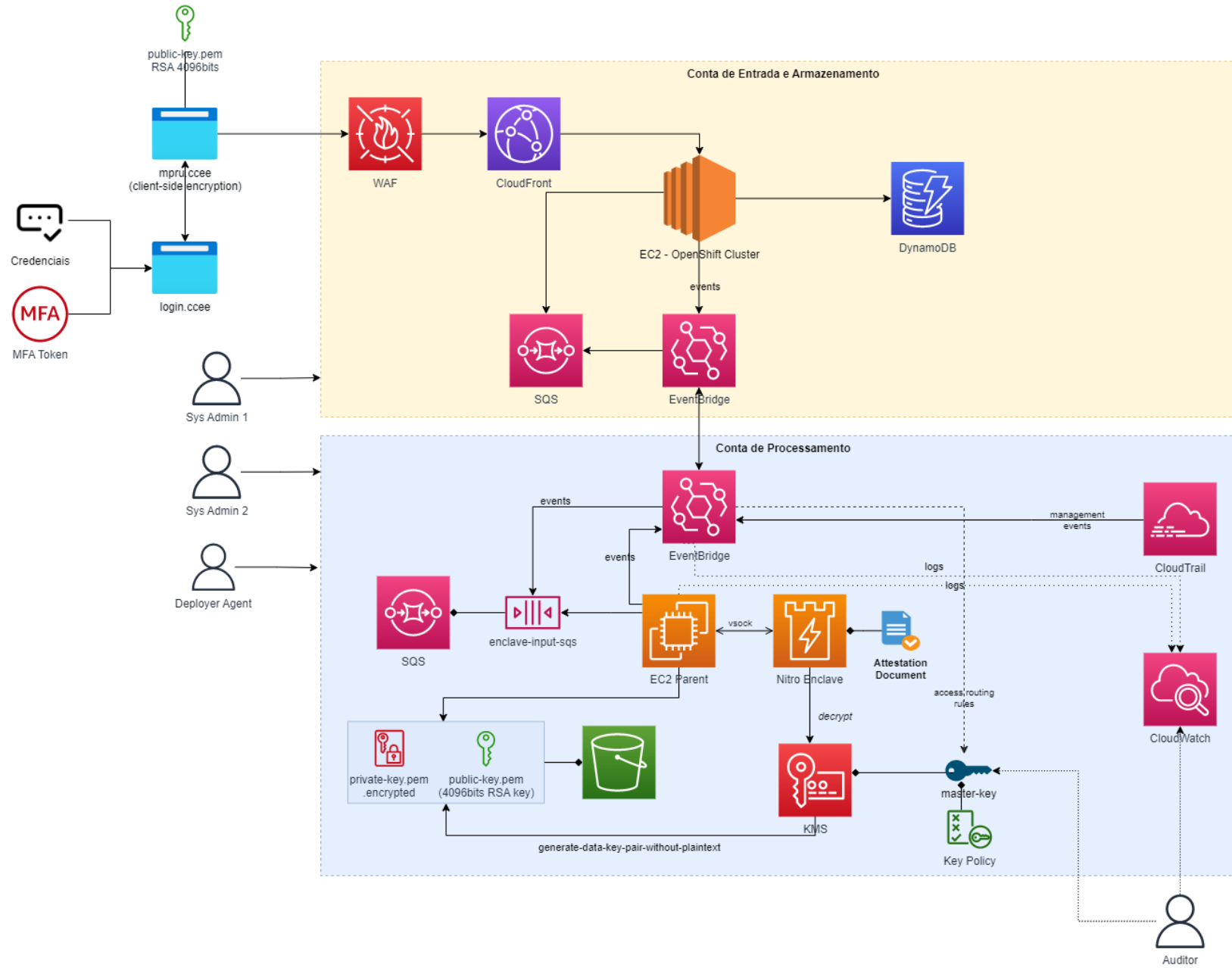


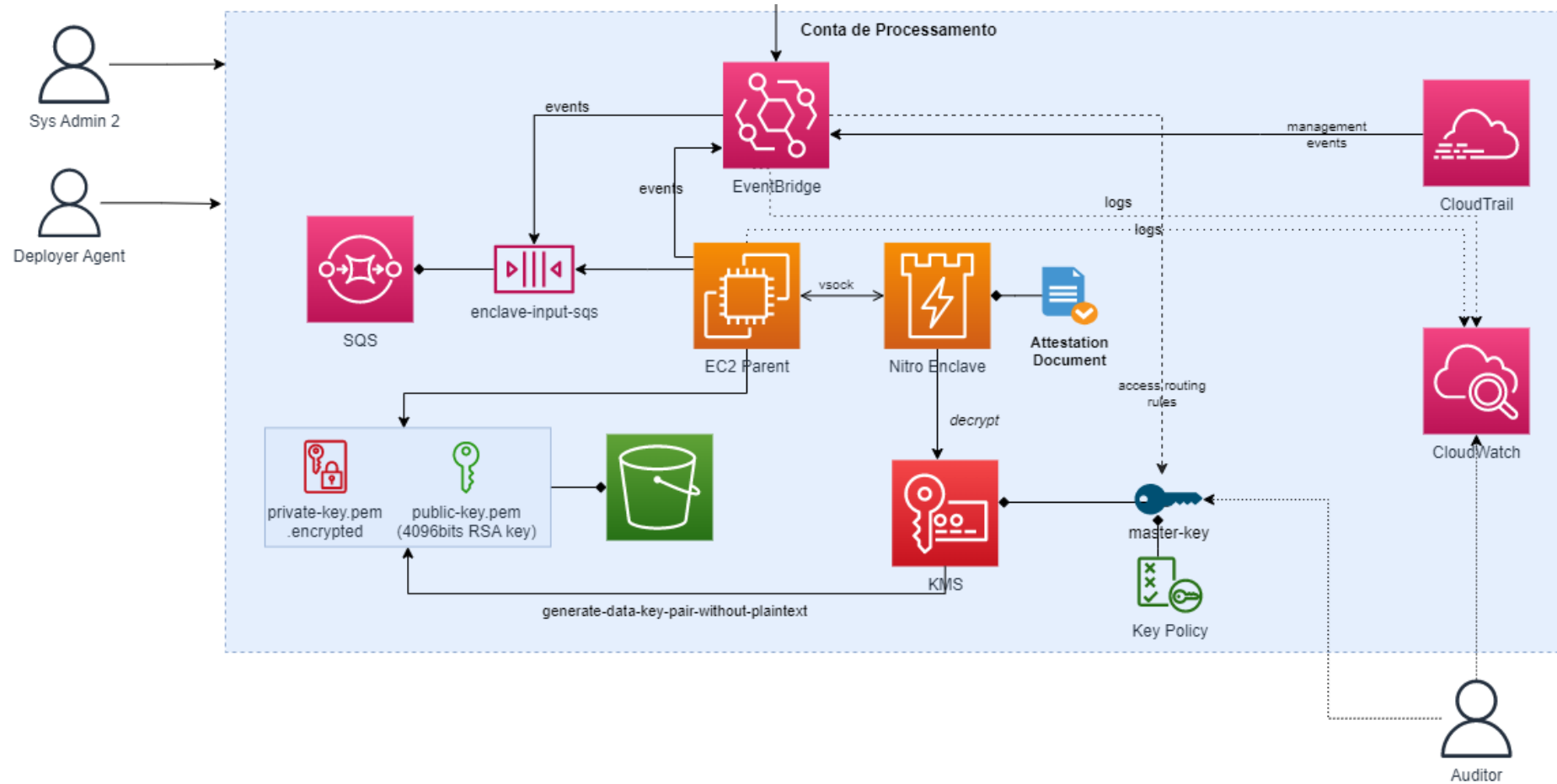


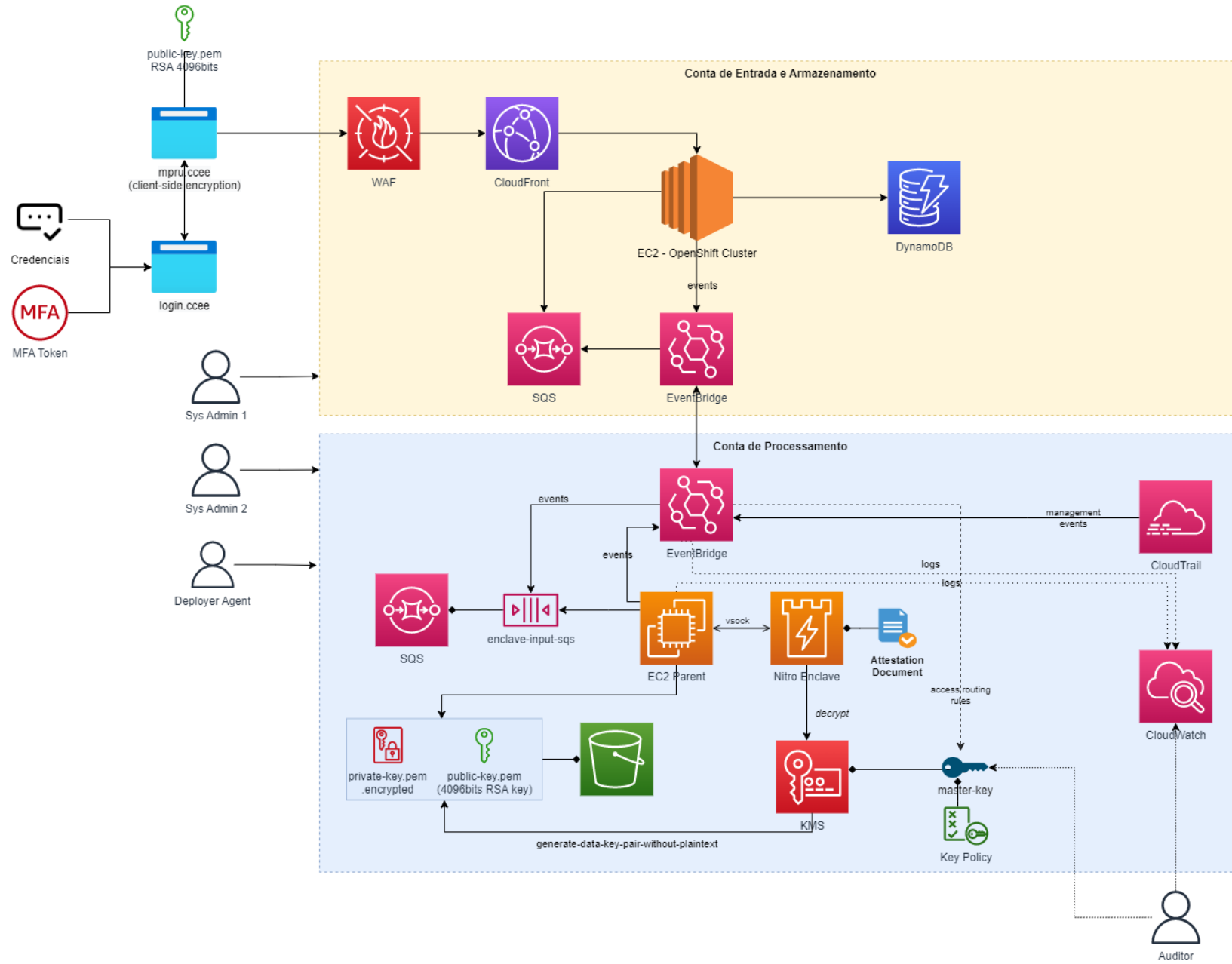
- Segregação de funções e políticas de mínimo privilégio
- Esteira automatizada para implantação de software nos ambientes de computação confidencial sem manipulação humana
- Certificação do código-fonte assegurando a inexistência de “backdoors”
- Auditoria de operações e alerta de alterações no ambiente











Segurança, Disponibilidade e Escalabilidade

MARCELO MOLINA