Relatório SGC Challenge

Armazenamento e Verificação de Múltiplas Assinaturas:

O sistema foi projetado para suportar múltiplas assinaturas em um único documento. Cada operador no sistema tem um objeto associado, que é uma instância da classe `Operador`. Esta classe contém, como atributos privados, o par de chaves (pública e privada), o certificado digital do operador e a assinatura criada usando a chave privada.

As assinaturas são armazenadas internamente na classe `Operador`. Quando um operador assina o documento, ele gera uma assinatura do hash do documento utilizando sua chave privada e armazena essa assinatura em sua instância.

Para verificar as assinaturas, o programa verifica, para cada operador, se a assinatura armazenada em sua instância coincide com a assinatura do hash do documento usando sua chave pública. Se todas as assinaturas forem válidas, pode-se afirmar que todos os operadores assinaram o documento e concordaram com seu conteúdo.

Funcionamento na Prática:

Na prática, o sistema serviria como um protocolo de acordo digital. Imagine uma situação onde múltiplas partes (operadores) precisam concordar com o conteúdo de um documento. Cada operador seria equipado com seu par de chaves e um certificado digital, que atesta a autenticidade de sua chave pública.

Os operadores se apresentariam ao sistema um por um. Cada operador, ao decidir concordar com o conteúdo do documento, assinaria o documento usando sua chave privada. Esta assinatura, juntamente com o certificado digital do operador, serve como uma prova irrefutável de que o operador concorda com o conteúdo do documento.

No programa, a construção do certificado digital de cada operador é feita dentro do construtor da classe `Operator`. Onde são definidas a chave pública, um número de série que o identifica, sua validade e informações sobre o titular do certificado. Então o certificado é assinado usando a chave privada do operador e um algoritmo de hash, no caso, SHA-256. A assinatura serve para atestar que o certificado foi emitido por uma autoridade confiável (neste caso, o próprio operador).

Execução da Aplicação:

A aplicação é iniciada através da linha de comando, onde é necessário fornecer o caminho do documento PDF que se deseja assinar: `./challenge.out <caminho_do_pdf>`.

Uma vez iniciado, o programa pede ao usuário para definir o número total de operadores. Após a definição, o programa entra em um loop, oferecendo três opções: assinar o documento, verificar as assinaturas ou fechar o sistema.

Para assinar o documento, um operador se identifica e usa sua chave privada para assinar o hash do documento. Esta assinatura é então armazenada na instância do operador.

Para verificar as assinaturas, o sistema percorre cada operador e verifica se sua assinatura é válida. Se todas as assinaturas forem válidas, indica que todos os operadores assinaram o documento e entraram em acordo.