

Desafio Etapa 5 - Relatório das Atividades

Matheus Cadorin

Ao longo do código, existem diversos comentários para facilitar a compreensão. Pesquisei muito sobre a Bouncy, Maven e SpringBoot e também precisei me basear em alguns trechos de código do Stack. Tive algumas dificuldades com o formato que os dados devem ser tratados. Pelos meus testes o desafio está completo.

Etapa 1 - Obtenção do resumo criptográfico (hash)

Aqui eu usei o OnlineTools para obter o hash do conteúdo do arquivo doc.txt.

Etapa 2 - Realizar uma assinatura digital

Usei o programa KeyStore Explorer para ter acesso às informações do certificado e poder validar meus métodos de acordo com os valores das variáveis.

Depois de procurar por alguns exemplos, entendi como iniciar e retirar o certificado (sua chave pública X509). Na retirada da chave, não conseguia fazer funcionar até testar com o typecast (para transformar o conteúdo do meu getCertificate/getKey no tipo que preciso (X509 ou PrivateKey)). Para criar o assinador da Bouncy, existiam exemplos prontos. Fazia os testes pelo console antes de implementar os endpoints.

Etapa 3 - Verificar a assinatura gerada

As instruções passadas nesta etapa foram vitais para que eu encontrasse uma maneira de resolver esta etapa. O maior desafio foi entender como obter e percorrer a lista de assinantes com o getSID do assinante, parte que eu gostaria de ter entendido melhor. Depois de alguns ajustes (nesta e na Etapa2), retornou true.

```
1 STATUS: Assinatura válida
```

Etapa 4 - API REST

Achei bem interessante esta parte. Reuni com um colega de classe que está aprendendo SpringBoot (para o processo seletivo de outra empresa) para estudarmos juntos. Basicamente aqui criei os endpoints (que são métodos do controlador da API) e defini a comunicação para que o Postman pudesse conversar com meu código enviando os parâmetros corretos que defini. Tive dificuldade no formato dos arquivos. O uso do Boot Dashboard facilitou bastante.

Fico à disposição!

Atenciosamente,
Matheus Cadorin