

Desafio Aplicativo Móvel

Desenvolver uma aplicação móvel (iOS ou Android) utilizando a ferramenta [Flutter](#) do Google.

A aplicação deve ter duas funcionalidades:

1. Listar dispositivos Bluetooth Low Energy (BLE) próximos.
2. Realizar operações criptográficas utilizando o algoritmo RSA: gerar um par de chaves RSA, assinar a lista de dispositivos usando a chave privada e verificar a assinatura gerada.

O aplicativo deve conter as seguintes telas, cujas sugestões de layout estão ilustradas na Figura 1.

- Tela 1: Uma tela inicial ao abrir o aplicativo. Deve possuir os botões "Dispositivos BLE", "Gerar chave RSA", "Assinar lista" e "Verificar assinatura".
- Tela 2: Acessível através do botão "Dispositivos BLE" da Tela 1. **Deve mostrar a data e hora da última varredura** por dispositivos BLE e os dispositivos encontrados. O botão "Atualizar lista" permite realizar uma nova varredura. O botão "Voltar" leva à Tela 1.
- Tela 3: Acessível através do botão "Gerar chave RSA" da Tela 1. Deve mostrar os dados do último par de chaves gerado (inicialmente nulo). O botão "Gerar nova chave" leva à Tela 4. O botão "Voltar" leva à Tela 1.
- Tela 4: Permite gerar um novo par de chaves substituindo o par anterior. Deve permitir ao usuário informar um número natural como tamanho do par de chaves a ser gerado. O botão "Voltar" leva à Tela 3, que deve ser atualizada com os dados da última chave gerada.
- Tela 5: Acessível via botão "Assinar lista" da Tela 1. Permite assinar a lista de dispositivos BLE gerada na Tela 2. Para assinar, você deve utilizar os algoritmos SHA256 e RSA. Após realizada a assinatura, deve-se atualizar a Tela 5 mostrando a assinatura digital codificada em formato Base64. O botão "Voltar" leva à Tela 1.
- Tela 6: Acessível via botão "Verificar assinatura" na Tela 1. O botão "Verificar novamente" verifica se a assinatura é válida e mostra o resultado da verificação na Tela 6. O botão "Voltar" leva à Tela 1.

Lembramos que a Figura 1 apresenta sugestões de layout. Incentivamos você a melhorá-las desde que não suprima quaisquer dados ou funcionalidades acima descritos.

Recomendamos a utilização de bibliotecas prontas de flutter/dart para a implementação das funcionalidades, como a biblioteca **FlutterBlue**, **Pointy Castle (ou Fast RSA)**, ou quaisquer outras que o(a) aluno(a) julgar necessário.

Por fim, você deve escrever um relatório de 2 a 5 páginas em formato PDF sobre o desenvolvimento da aplicação. Nesse relatório você deve descrever as tarefas realizadas e os desafios encontrados **mesmo que você não consiga finalizar o desafio**. Isso porque, estamos interessados em avaliar não só seu grau de conhecimento, mas também sua dedicação em resolver o desafio, organização de código, etc. Adicionalmente, você deve descrever tudo que precisamos saber para executarmos seu aplicativo móvel.



Figura 1 - Sugestão de layout de telas.