

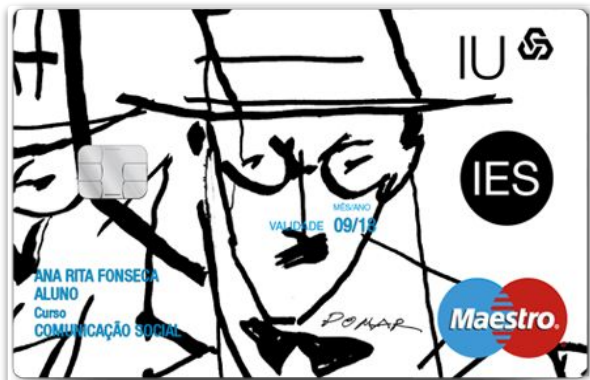




ÍNDICE :

1. Contextualização do produto;
2. Gestão da Equipa;
3. Arquitetura da solução;
4. Pontos críticos da solução;
5. Infraestrutura para produção;
6. Reflexão crítica sobre o projecto.

Identificação



Serviços





Gestão da Equipa



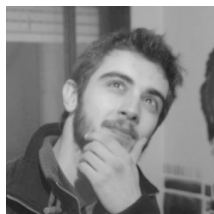
Security



Mateus Ferreira



Diogo Duarte



Ricardo Dias

Database



Rui Rodrigues



Nuno Valente

BackEnd



Pedro Ferreira



Alexandre Rodrigues

FrontEnd



Filipa Parente



Leonardo Silva



CTO



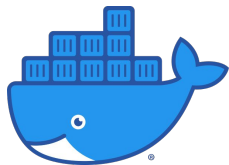
CEO



Consultor

Security

CA



Database

CA



IA



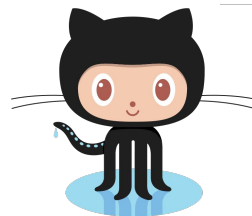
BackEnd



FrontEnd

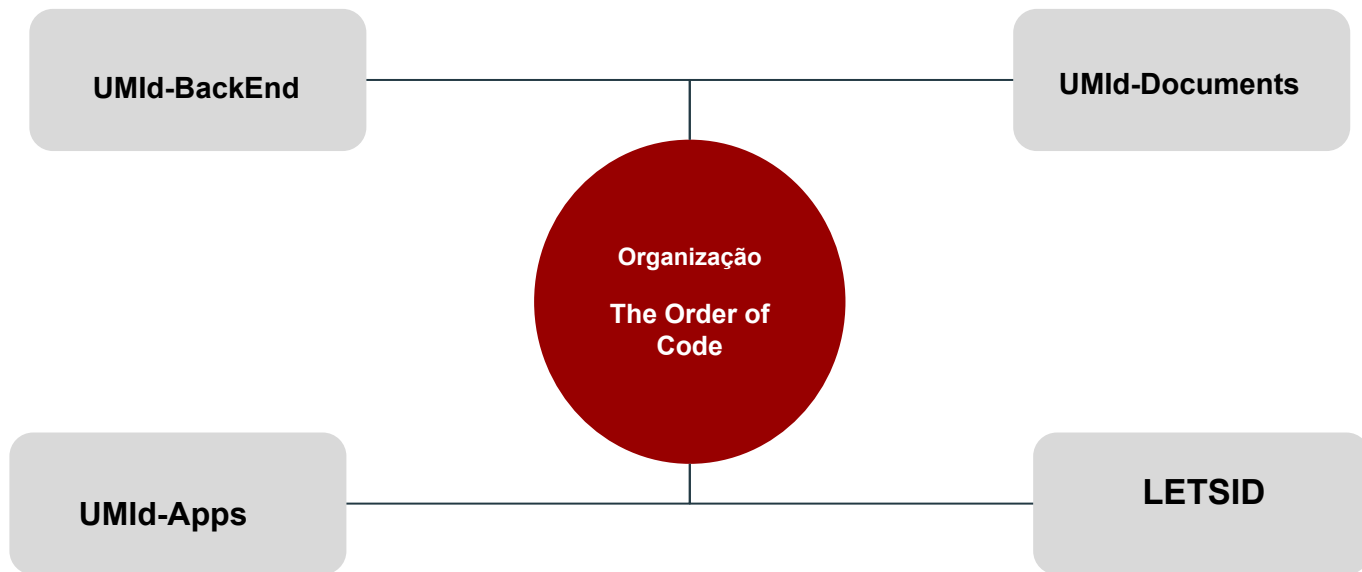


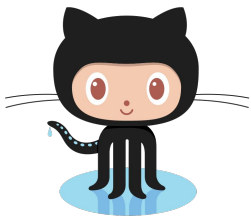
Management



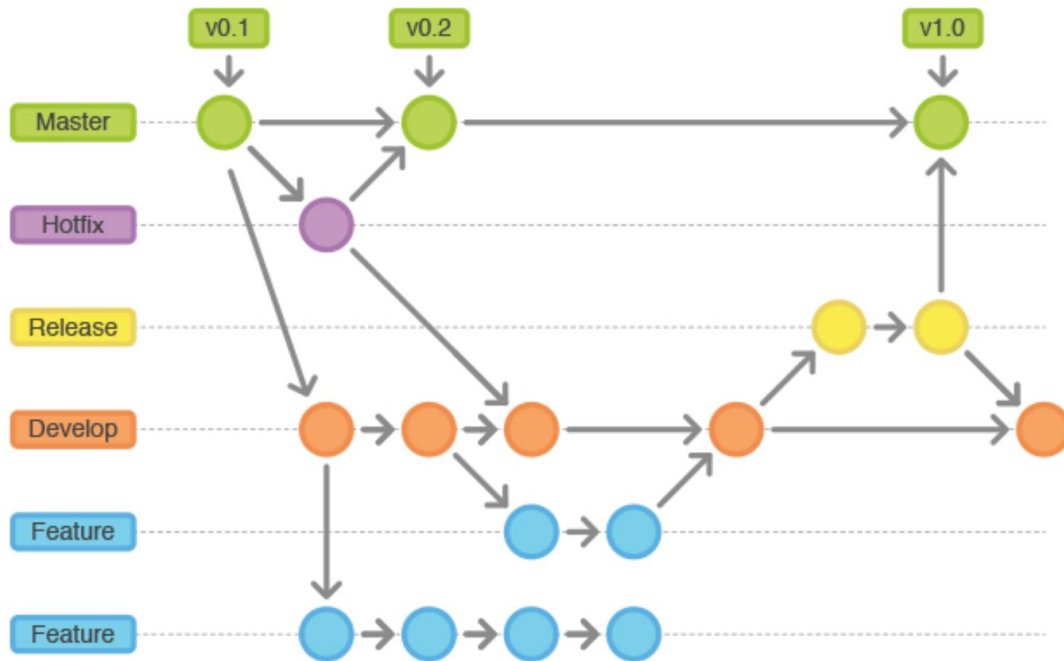


Para organização do desenvolvimento foi criado uma estrutura no GitHub que refletisse a divisão das sub-equipas.





A gestão dos repositório foi utilizado a metodologia Git-Flow.

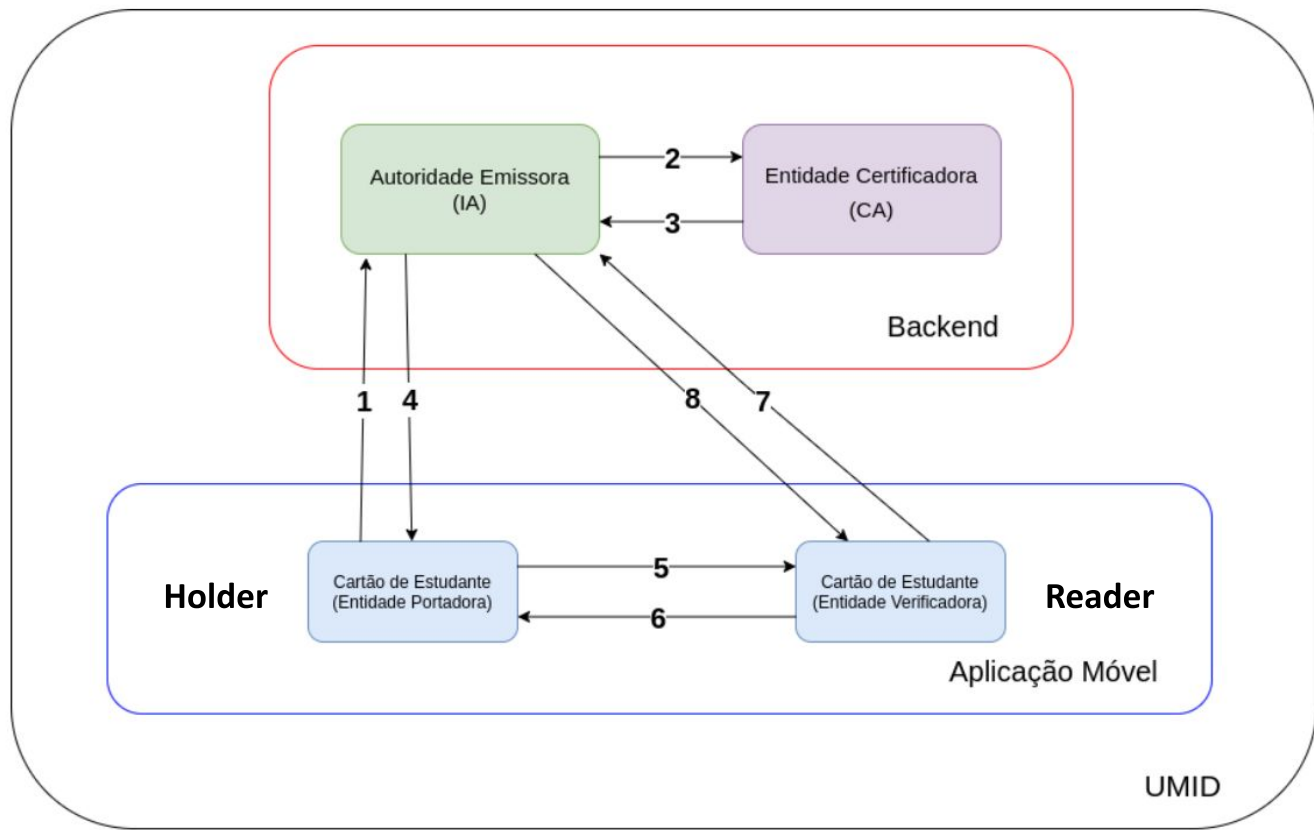




1. Reuniões ocorrem em sua maioria aos sábados;
2. As sub-equipas tiveram liberdade de se auto gerenciarem, dentro do tempo da tarefa atribuída a eles.



Arquitetura da Solução





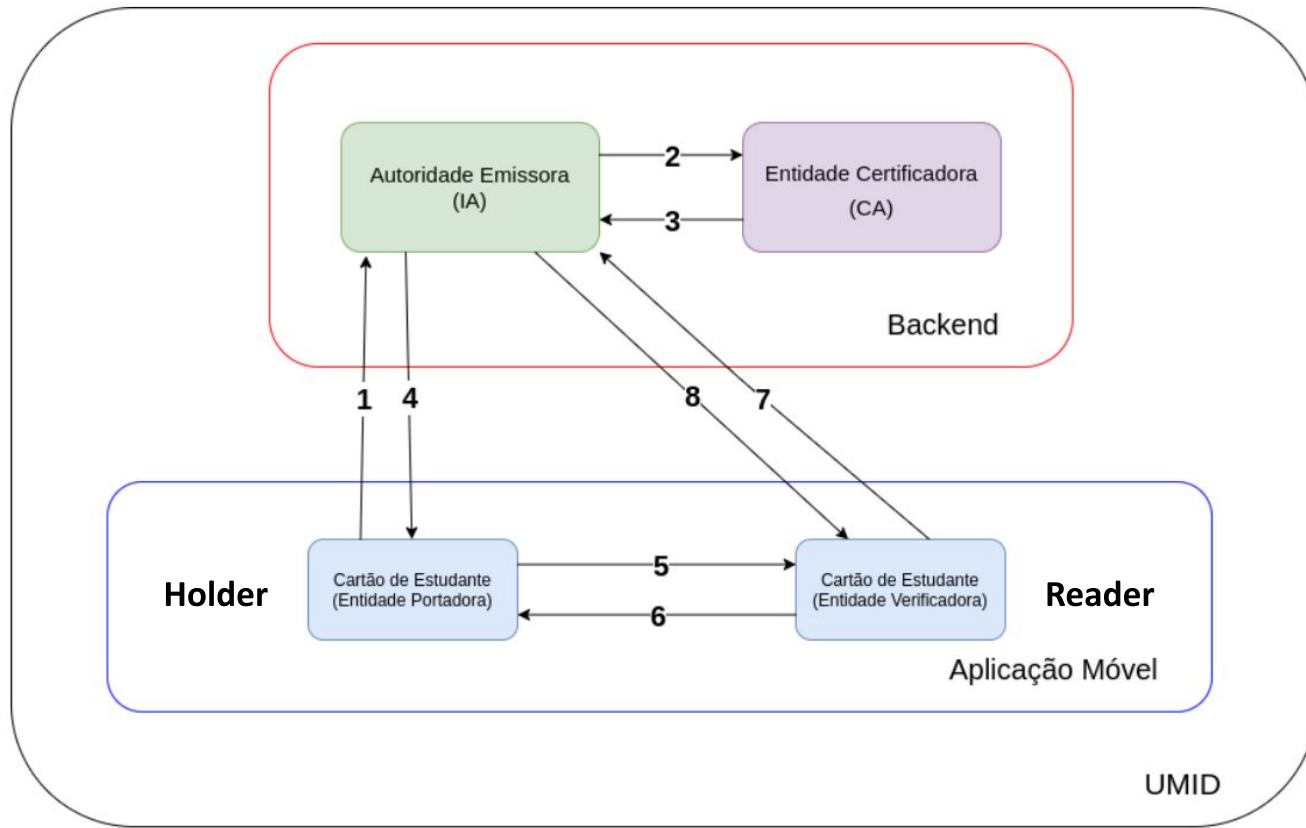
Pontos Críticos da Solução



Requisitos não funcionais (Segurança):

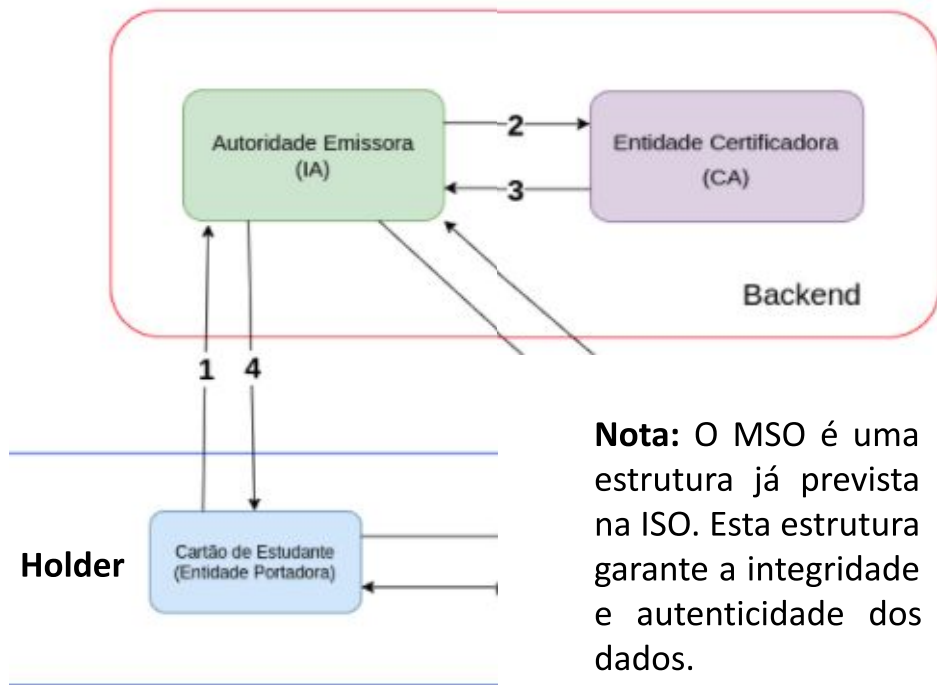
- Requisito nº40: Os dados transferidos devem ser autênticos, íntegros e confiáveis; (Must)
- Requisito nº41: O produto deve rejeitar a receção de dados inválidos; (Must)
- Requisito nº43: O produto deve proteger as informações privadas de acordo com as leis de privacidade relevantes e a política de informações da organização. (Must)

Estes requisitos encontram-se explícitos no standard ISO/IEC DIS 18013-5.





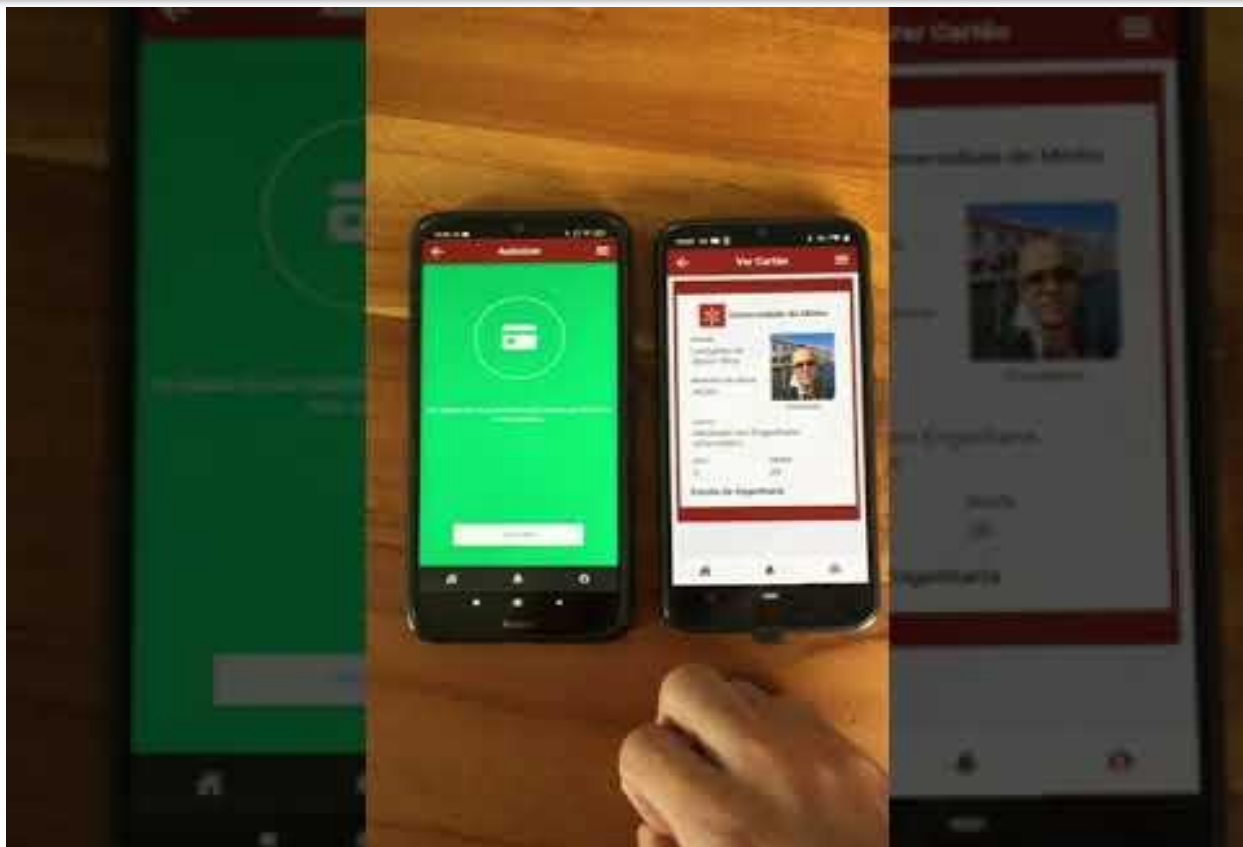
Relação entre Autoridade Emissora e Entidade Portadora:



Nota: O MSO é uma estrutura já prevista na ISO. Esta estrutura garante a integridade e autenticidade dos dados.

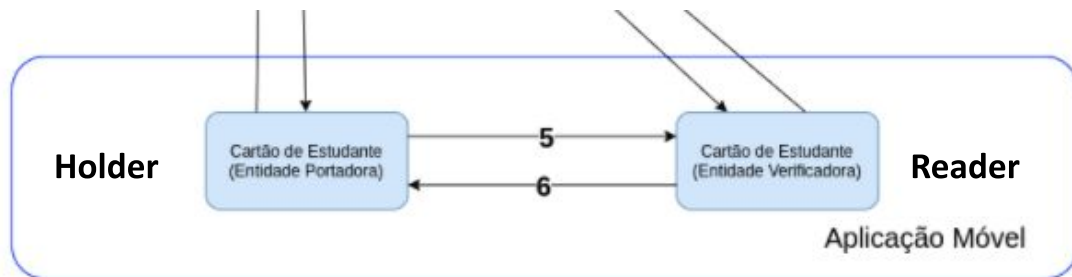
O processo de associação de um cartão na aplicação divide-se em 4 passos:

1. Envio de um CSR e dos dados de autenticação para a IA;
2. Envio do CSR da IA e da estrutura do cartão para a CA;
3. Envio do certificado gerado e do MSO à IA (ver Nota);
4. Envio do certificado gerado, do MSO e dos dados associados ao Holder.





Relação entre Entidade Portadora e Entidade Verificadora:



5. Device Engagement

- O Holder apresenta um QR-Code com os dados necessários para o estabelecimento da sessão segura de transferência;
- O Reader lê o QR-Code e estabelece uma sessão segura entre as duas entidades.

6. Data Retrieval

- O Reader envia um pedido ao Holder com os dados que pretende;
- O Holder recebe o pedido e, mediante o consentimento do utilizador final, envia ou não os dados pretendidos;
- Validação dos dados provenientes do Holder..



Relação entre Entidade Verificadora e Autoridade Emissora:

A norma ISO contempla dois tipos de data retrieval:

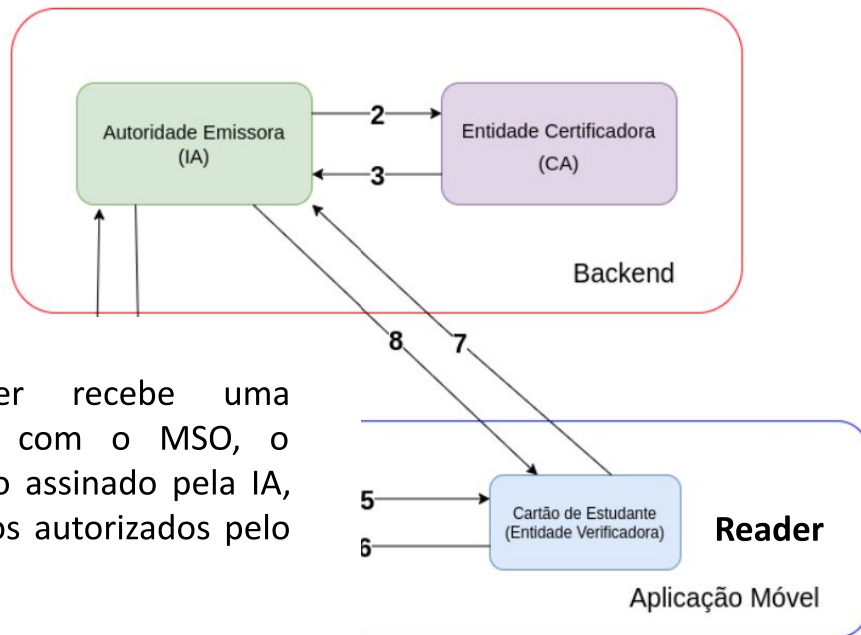
- Via **Autoridade Emissora (IA)**, constituindo o modo online de obtenção dos dados;
- Via **Holder**, constituindo o modo offline de obtenção dos dados;

Via **Autoridade Emissora:**

- o Reader recebe um token do Holder contendo o Identificador do Cartão e os namespaces dos atributos que autorizou o Reader a aceder.

Via **Holder:**

- o Reader recebe uma estrutura com o MSO, o certificado assinado pela IA, e os dados autorizados pelo Holder.





Infraestrutura para produção

Infraestrutura para Produção:



Google Cloud

Para montar a Infraestrutura da Autoridade Emissora (IA):

- Criar 2 instâncias no Google Cloud Platform;
- Numa das instâncias, correr o docker-compose com a configuração da CA e da BD da CA;
- Na outra instância:
 - Configurar o endereço IP da CA;
 - Correr o servidor Django com a simulação da IA da Universidade do Minho.



Infraestrutura para Produção:



Nota: É necessário que o dispositivo possua um método de segurança (PIN, biometria, padrão, etc.)

Para o build das aplicações móveis:

- Instalar a framework Ionic, preferencialmente num computador com sistema operativo Mac OSX (para fazer build das apps para iOS);
- Fazer clone do repositório:
(<https://github.com/The-Order-of-Code/UMId-Apps>);
- Ir para a diretoria UMIdAPP e executar os seguintes comandos:
 - `npm i` (para instalar as packages do nodejs necessárias);
 - `ionic cordova prepare android/ios` (para gerar o código nativo);
 - `ionic cordova build android/ios` (para gerar as aplicações).



Reflexão crítica do projecto



Trabalho futuro:

Aspetos a melhorar:

- Adição de novas funcionalidades (marcação de presenças, parquímetros, gestão de eventos, etc.);
- Criação de um plugin personalizado para a comunicação BLE;
- Integração da aplicação móvel com os serviços da Universidade do Minho;
- Adição de novos meios de comunicação para a transferência de dados (NFC e Wifi Aware);



Let's



Filipa Parente A82145
Rui Rodrigues A74572
Nuno Valente A81986
Pedro Ferreira A81403
Ricardo Dias PG39295
Diogo Duarte PG41843
Leonardo Silva PG39261
Mateus Ferreira PG37159
Alexandre Rodrigues A81451

guia para montar apresentação / este slide será retirado
ao fim

Apresentação técnica

1 - Breve conceptualização da solução (Leo)

2- Arquitetura da solução (Leo)

3- slides pontos críticos (requisitos não funcionais) - falar definição PIN (Filipa)

**4 - gitflow/coordenação da equipa / gestão de equipa / lado dos
componentes (Leo)**

5 - a infraestrutura para colocar em produção (Filipa)

6 - reflexão crítica da abordagem utilizada (Filipa)