Tutorial para usar certificado digital no CDDL

1 - Criar chave raiz

Atenção: esta é a chave utilizada para assinar os pedidos de certificado, qualquer pessoa que a possua pode assinar certificados em seu nome. Portanto, mantenha-o em um lugar seguro!

```
openssl genrsa -des3 -out rootCA.key 4096
```

Se você quiser uma chave não protegida por senha, basta remover a `-des3` opção

2 - Criar e autoassinar o certificado raiz

Insere as informações necessárias do certificado (País: br, Estado: ma, Localidade: slz, Organização: ufma, Unidade organizacional: LSDi, Nome Completo: Autoridade certificadora do LSDi e E-mail: ca@lsdi.ufma.br) e senha(123456)

```
openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out
rootCA.crt
```

Aqui, usamos nossa chave raiz para criar o certificado raiz que precisa ser distribuído em todos os computadores que precisam confiar em nós.

3 - Levar os arquivos `rootCA.key e rootCA.crt para o smartphone do usuário que terá permissão. DICA: emulador(usa google drive), smartphone físico (cabo usb)`

4 - Na classe do projeto MainActivity.java, insere o código:

```
SecurityService securityService = new SecurityService( getApplicationContext() );
securityService.generateCSR("jean","LSDi","ufma","slz","ma","br");

Obs: será gerado um arquivo client.csr, trata-se de uma requisição feita para CA,
para assinar o certificado.
```

5 - Gerou um arquivo client.csr na pasta Download, agora leva para o desktop para a Autoridade Certificadora (CA) assinar. Leva o arquivo para google drive e faz o download do arquivo.

6 - No prompt de comando, execute a linha:

```
openssl x509 -req -in client.csr -CA rootCA.crt -CAkey rootCA.key
-CAcreateserial -out  client.crt -days 500 -sha256
```

7 - Depois de gerado o arquivo client.crt, que é o certificado assinado pela CA, leva-o para o smartphone através do google drive, e baixe-o colocando na pasta download do smartphone. Execute o código abaixo.

```
String nameCaCertificate = "rootCA.crt";
String nameClientCertificate = "client.crt";



SecurityService securityService = new SecurityService( getApplicationContext() );
//securityService.generateCSR("jean","LSDi","ufma","slz","ma","br");
try {
   securityService.setCaCertificate(nameCaCertificate);
   securityService.setCertificate(nameClientCertificate);

   securityService.grantReadPermissionByCDDLTopic("lcmuniz@gmail.com",SecurityServi
   ce.ALL_TOPICS);
   securityService.grantWritePermissionByCDDLTopic("lcmuniz@gmail.com",SecurityServ
   ice.ALL_TOPICS);

} catch (FileNotFoundException e) {
   e.printStackTrace();
}
```

8 - Pronto!, está criado e assinado o certificado digital do cliente pela CA.