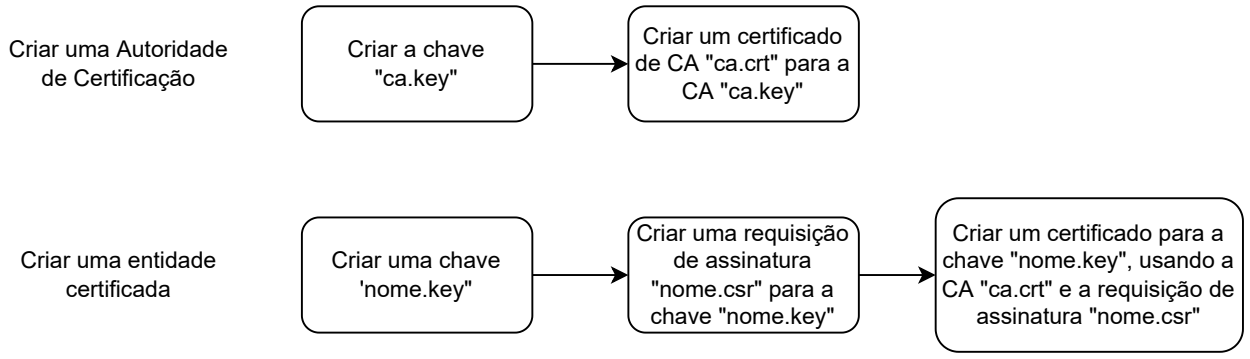
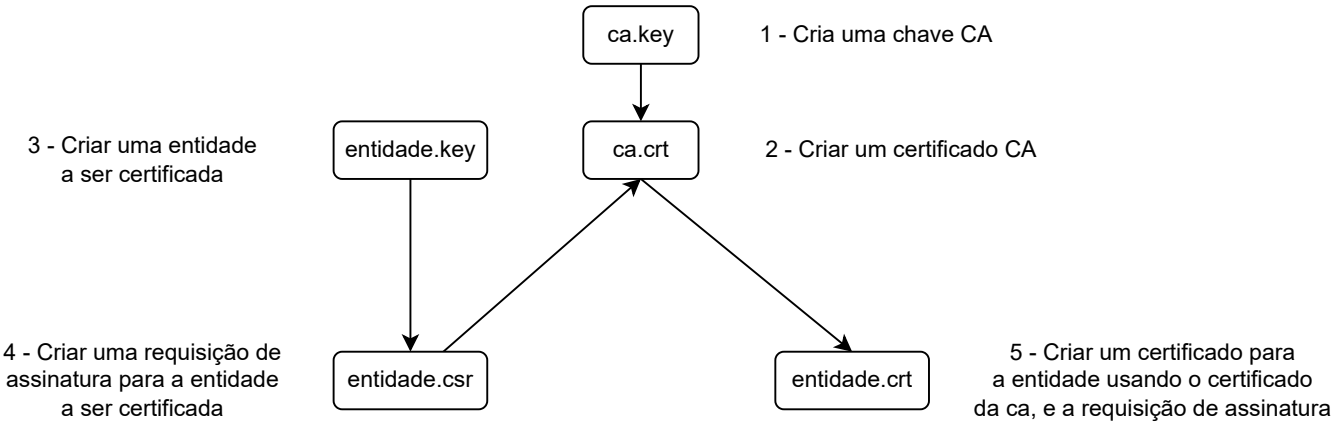
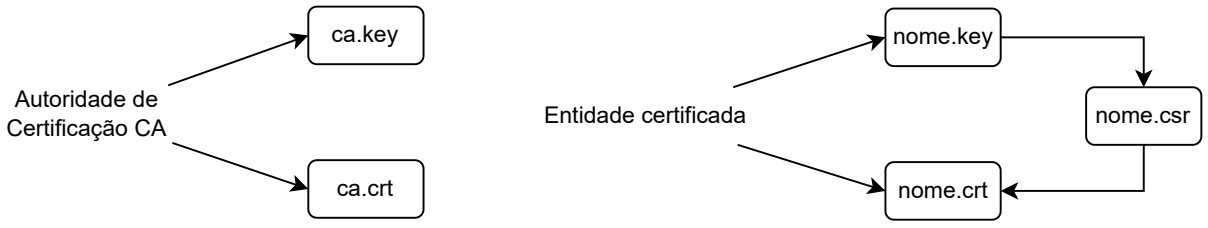
SSL Server - Fluxo Operacional

Descrição: Fluxo operacional de um sistema protegido por ssl

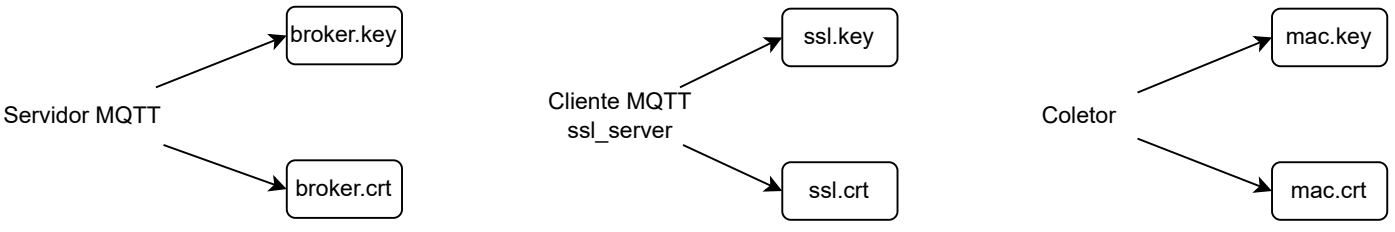




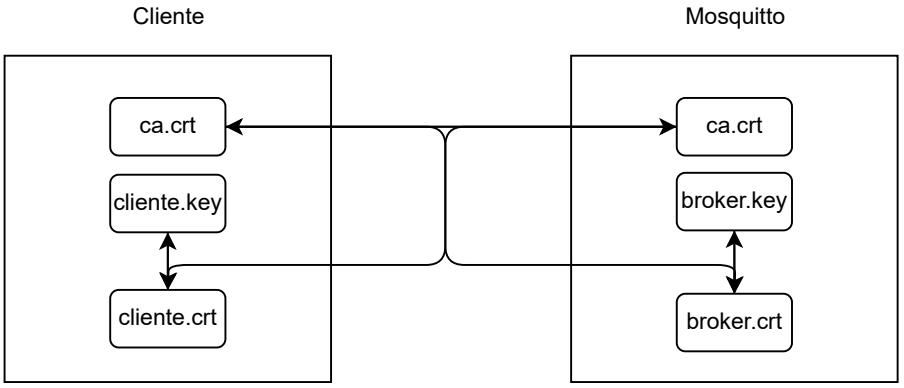
A requisição de assinatura entidade.csr vai possuir vários dados de autenticação, sendo os principais o CN, e o passphrase. O CN é o nome da entidade, que deve preferencialmente ser um nome de domínio. No caso do servidor mqtt por exemplo, o CN DEVE ser o nome de domínio do próprio servidor, pois no momento da autenticação, a CA irá verificar se o certificado do servidor está com o CN correto. E o passphrase deve ser a senha usada no momento de criar o certificado da CA. Pois do contrário, a requisição de assinatura não será concluída pela CA.



Exemplos de possíveis entidades certificadas:



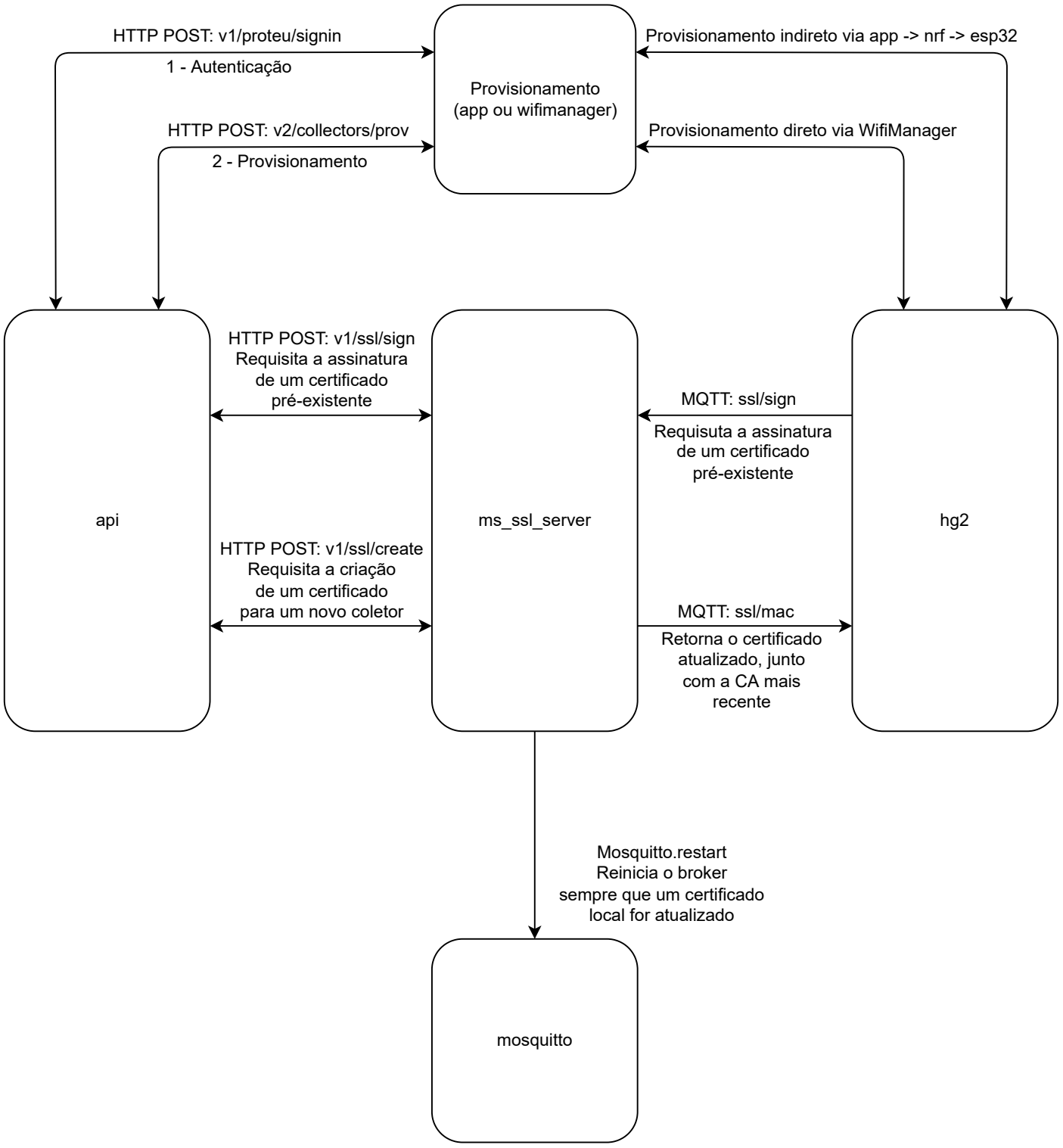
A CA (Autoridade de Certificação) sempre irá realizar a autenticação entre o servidor e o cliente. O fluxo de autenticação é descrito abaixo:



Primeio é verificado se os certificados das CAs são da mesma autoridade de certificação. Depois, é verificado se os certificados client.crt, e broker.crt, estão assinando as chaves client.key, e broker.key. Também é verificado o prazo de validade da assinatura, e se a assinatura foi feita pela mesma autoridade de certificação, no caso representada pelo certificado CA.crt. Se as chaves forem auto-assinadas, ou seja, se o cliente assinou a própria chave, ou se o broker assinou a própria chave, e não a CA, a conexão é considerada insegura.

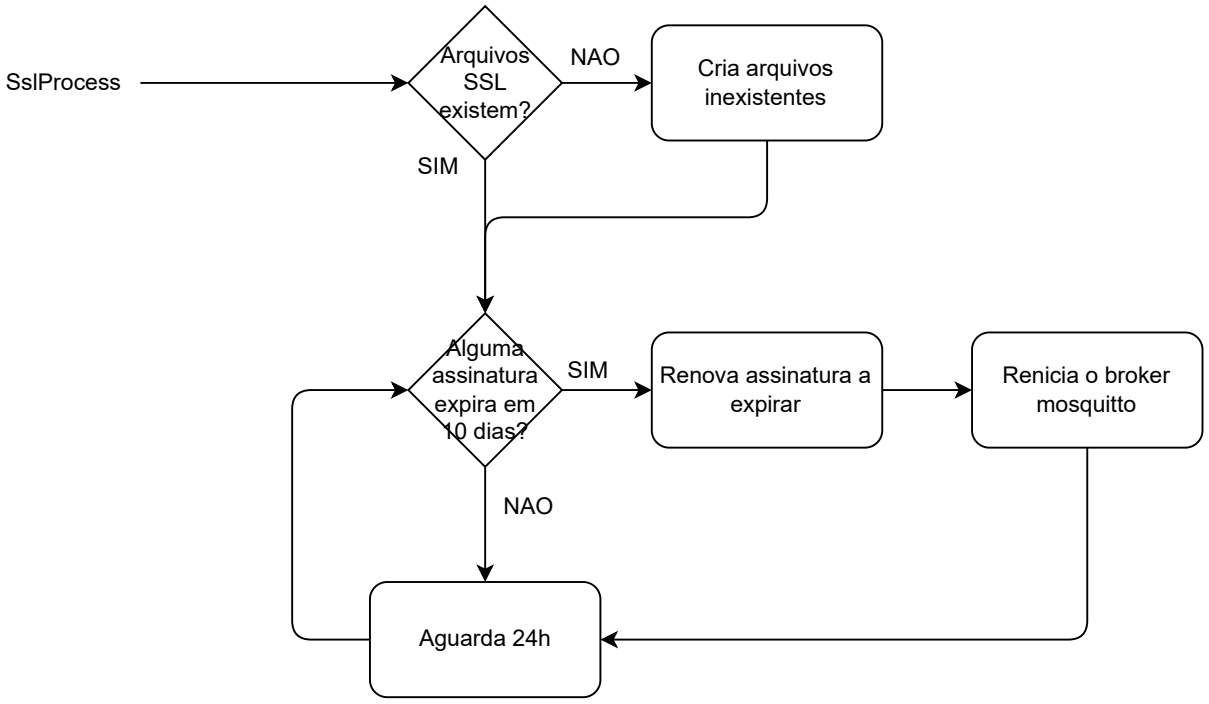
SSL Server - Arquitetura do Sistema

Descrição: Arquitetura proposta para integração dos sistemas envolvidos.



SSL Server - Fluxo lógico do Sistema

Descrição: Fluxo lógico proposto para integração dos sistemas envolvidos.



SSL Server - Rotas do Sistema

Descrição: Rotas utilizadas para comunicação do SSL Server com demais sistemas

HTTP POST: v1/ssl/sign MQTT SUB: ssl/sign

Corpo da requisição HTTP ou conteúdo publicado no tópico do MQTT:

```
{
    "name": "string",    //< Mac do coletor detentor do certificado a ser assinado
    "days": "string",    //< Prazo de validade da assinatura a ser realizada
    "pass": "string"     //< Senha da Autoridade de Certificação que irá realizar a assinatura
}
```

Resposta da requisição HTTP, ou conteúdo publicado no tópico de resposta do MQTT ssl/mac:

```
{
    "ca" : "string",     //< Autoridade de Certificação responsável pela assinatura do certificado
    "key" : "string",    //< Chave da entidade SSL
    "crt" : "string"     //< Certificado da entidade SSL assinado pela CA
}
```

HTTP POST: v1/ssl/create

```
{
    "name": "string",       //< Mac do coletor detentor do certificado da entidade SSL a ser criada
    "days": "string",       //< Prazo de validade da assinatura a ser realizada
    "pass": "string",       //< Senha da Autoridade de Certificação que irá realizar a assinatura
    "country": "string",    //< País da organização detendora da entidade SSL a ser criada
    "state": "string",      //< Estado da organização detendora da entidade SSL a ser criada
    "locality": "string",   //< Cidade da organização detendora da entidade SSL a ser criada
    "org": "string",        //< Organização detentora da entidade SSL a ser criada
    "unit": "string",       //< Unidade da organização detentora da entidade SSL a ser criada
    "cn": "string",         //< Nome de domínio da organização, a ser atrelado a entidade SSL criada
    "email": "string"       //< E-mail da organização detentora da entidade SSL a ser criada
}
```

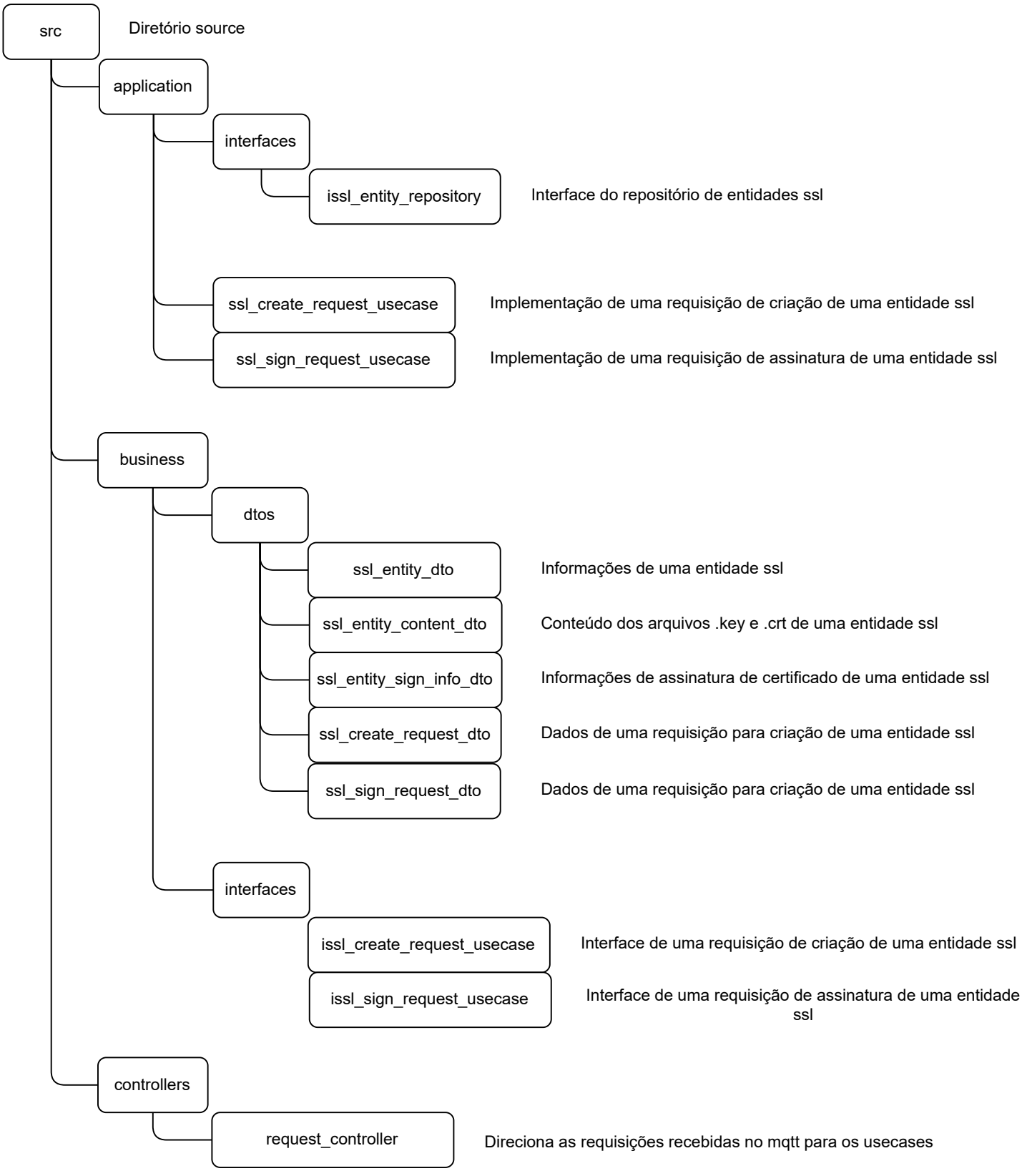
Resposta da requisição HTTP

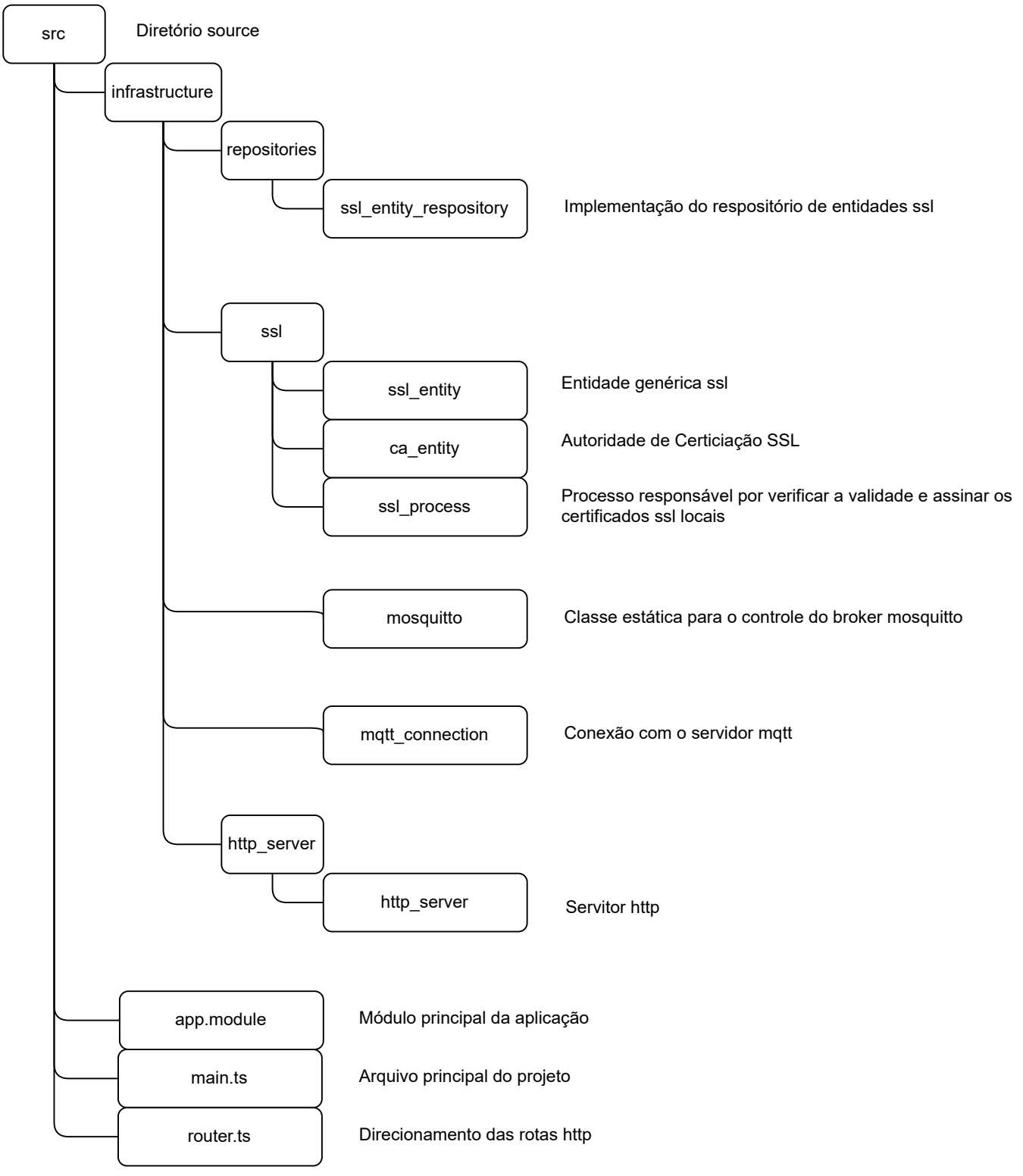
```
{
    "ca" : "string",     //< Autoridade de Certificação responsável pela assinatura do certificado
    "key" : "string",    //< Chave da entidade SSL
    "crt" : "string"     //< Certificado da entidade SSL assinado pela CA
}
```

Como especificado acima, a resposta das requisições será sempre a mesma.

ms_ssl_server

Descrição: Microservico responsável pelo gerenciamento dos certificados de segurança do servidor mqtt




src
Diretório source
infrastructure
repositories
ssl_entity_respository
Implementação do respositório de entidades ssl
ssl
ssl_entity
Entidade genérica ssl
ca_entity
Autoridade de Certiciação SSL
ssl_process
Processo responsável por verificar a validade e assinar os certificados ssl locais
mosquitto
Classe estática para o controle do broker mosquitto
mqtt_connection
Conexão com o servidor mqtt
http_server
http_server
Servitor http
app.module
Módulo principal da aplicação
main.ts
Arquivo principal do projeto
router.ts
Direcionamento das rotas http