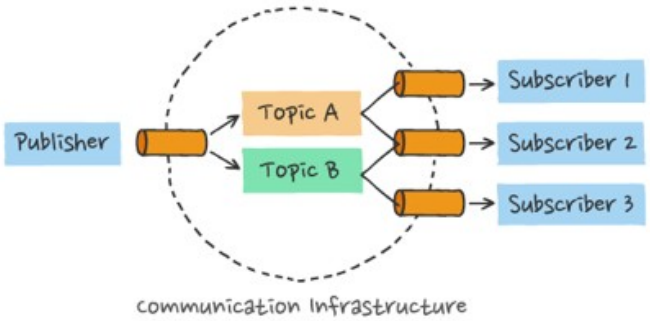
AVALIAÇÃO 3

1. IDENTIFICAÇÃO

CURSO: CIÊNCIA DA COMPUTAÇÃO **FASE:** 5ª **ANO/SEMESTRE:** 2025/1
DISCIPLINA: REDES DE COMPUTADORES II (RCB)
PROFESSOR: ROBSON COSTA **DATA:** 07/04/2024

Com base nos conceitos apresentados em aula e utilizando a linguagem de programação de sua preferência crie uma infraestrutura de comunicação (software cliente e *broker*) que opere de forma similar ao protocolo MQTT (*Message Queuing Telemetry Transport*), ou seja, no modelo *publish/subscriber*, mas com especificações de segurança e autenticação.



O ***broker*** é o responsável por gerenciar os tópicos existentes, receber solicitações de entrada ou saída de clientes de tópicos existentes, receber a solicitação de criação de um tópico por um cliente, receber a publicação de clientes em tópicos específicos bem como também autenticar e autorizar operações dos clientes no *broker*.

Os **clientes**, por sua vez, podem enviar solicitações de entrada em múltiplos tópicos de um único *broker*, enviar solicitações de publicação em tópicos específicos e também enviar solicitação de autenticação e autorização.

Toda a comunicação entre os clientes e o *broker* deve ser implementada sobre o **protocolo de transporte TCP**, para garantir a entrega e ordenação das mensagens. Além disso, para garantir confidencialidade de terceiros (ex.: ataques de *man-in-the-middle*) no fluxo de tráfego entre os clientes e o *broker*, este tráfego deve se **criptografado** utilizando uma técnica de envelopamento digital de implementação própria (não pode ser utilizado o protocolo TLS), conforme descrito em sala de aula. Para tal, os clientes precisam autenticar o certificado digital do *broker* o qual deve estar assinado pela AC (Autoridade Certificadora) que será o professor da disciplina.

Além de garantir um fluxo criptografado e autenticidade do *broker*, a infraestrutura também deve permitir a autenticação dos clientes que solicitam conexão. Conforme descrito em sala de aula, esta autenticação deve ocorrem com base na assinatura contida no Certificado Digital dos clientes, a qual deve ser realizada pelo *broker*, de forma similiar ao que ocorreu com a AC.

Além de garantir a confidencialidade contra terceiros, a infraestrutura também precisa garantir confidencialidade ponta a ponta. Neste caso em específico, apenas os nós comunicantes podem ter acesso ao conteúdo da mensagem (*payload*), ou seja, o *broker* não pode ser capaz de decodificar o conteúdo da mensagem, apenas o seu cabeçalho para poder encaminhá-la aos tópicos específicos. A criptografia ponta a ponta pode ocorrer de forma simétrica ou assimétrica. A estratégica pela sua adoção trata-se de uma decisão de projeto.

Abaixo segue um esquema gráfico onde são apresentados alguns fluxos: