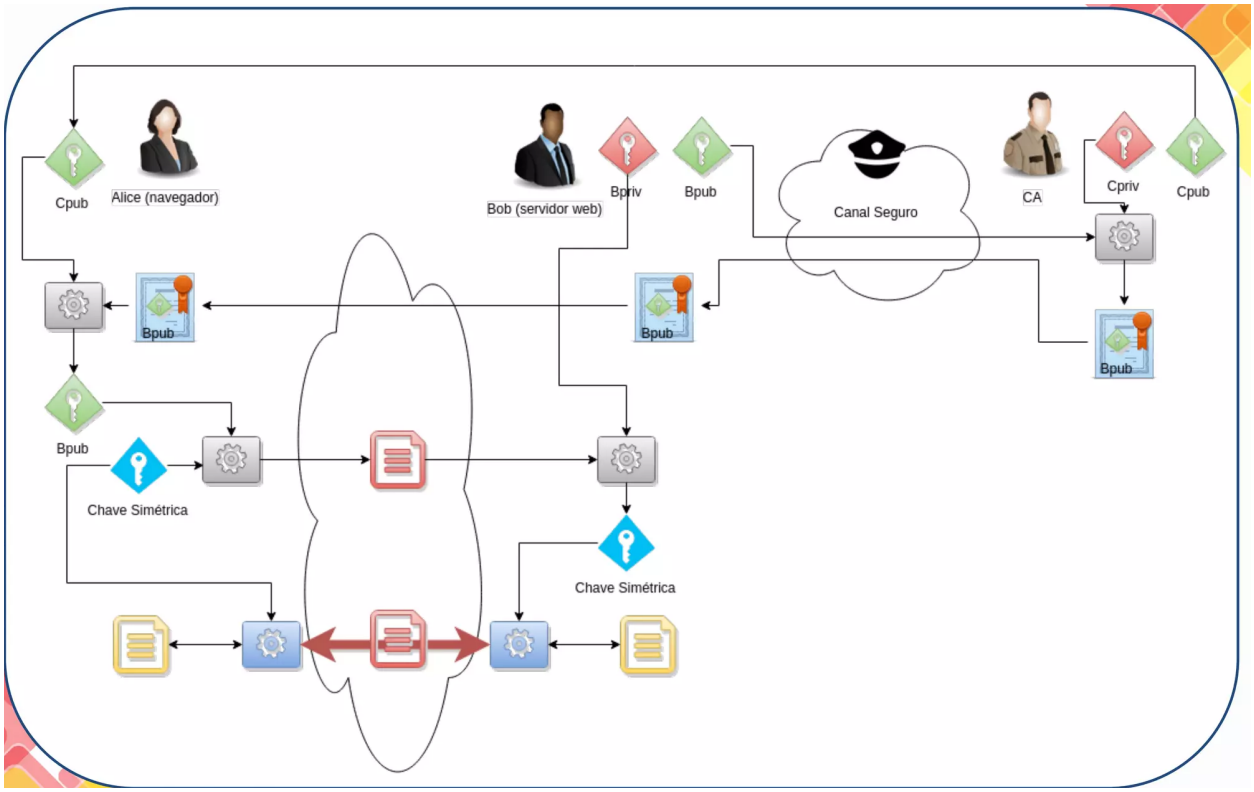
Curso: **TADS**	Semestre: **4º Noturno**
Disciplina: **Segurança de Software**	Professor: **Luiz Fernando**
Data: **10/07/2025**	
Aluno:	Nota:

AVALIAÇÃO – N2

1. Nesta atividade vocês implementarão o conceito de chave mista em uma infraestrutura com PKI, conforme a figura a seguir: **(10,0)**



Nesta atividade vocês farão o papel da Alice para comunicar comigo, que serei o Bob e a CA. Sendo assim, vocês devem baixar minha chave pública de CA, chave LuizSegato(Prova_CA) publicada no repositório keyserver.ubuntu.com com ID 013B9C5FF1B319E6. Após baixarem, vocês deverão usá-la para decifrar o certificado digital de Bob (disponível no moodle). Na sequência, deverão usar a

chave pública de Bob obtida de seu certificado para decifrar a chave simétrica (disponível no moodle) que será usada para comunicação de Alice e Bob daqui para frente. Ao decifrar esta chave vocês deverão usá-la para decifrar o último item deste processo, o texto que contém a mensagem que enviei a vocês (disponível no moodle). Ao final, vocês deverão encaminhar via moodle um print com o resultado de cada comando usado em cada etapa, desde quando baixaram a chave da CA no repositório até quando decifraram a mensagem final. Cuidado para não esquecer nenhum print, pois sua avaliação será em cima destes prints, cada informação que faltar vocês poderão perder nota.