Introdução a Certificação Digital: Conceitos Básicos

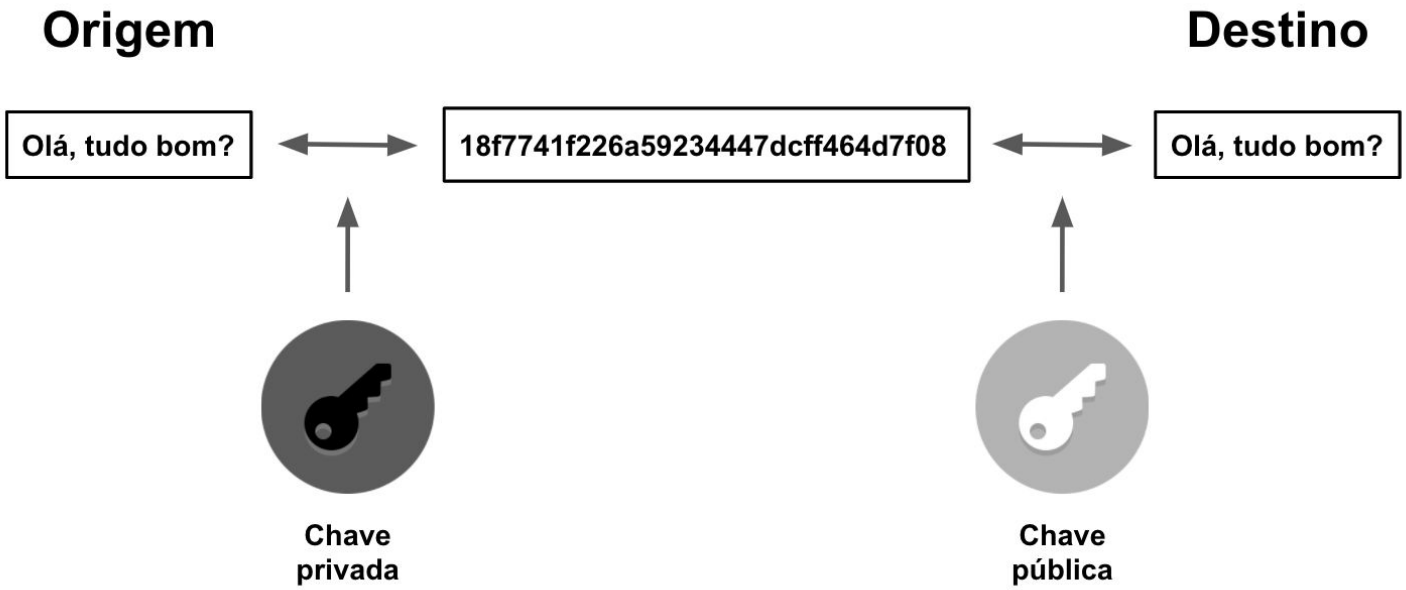
Professor Bsc. Lucas Mayr

Universidade Federal de Santa Catarina (UFSC)
Laboratório do Segurança e Computação (LabSEC)

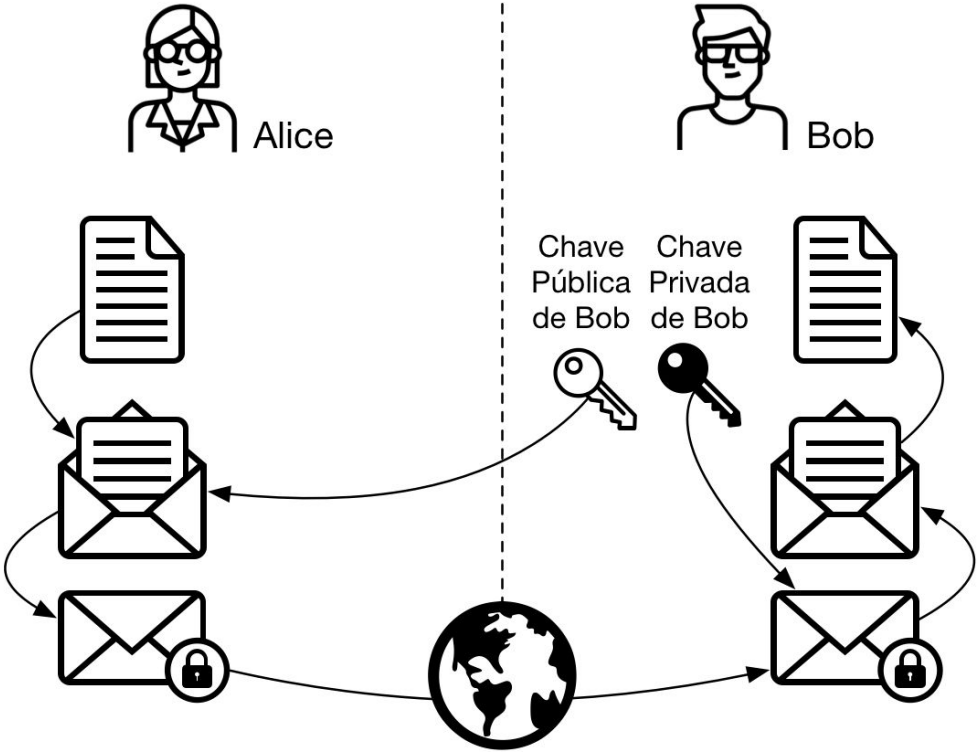
Março de 2023

Documentos Electrónicos

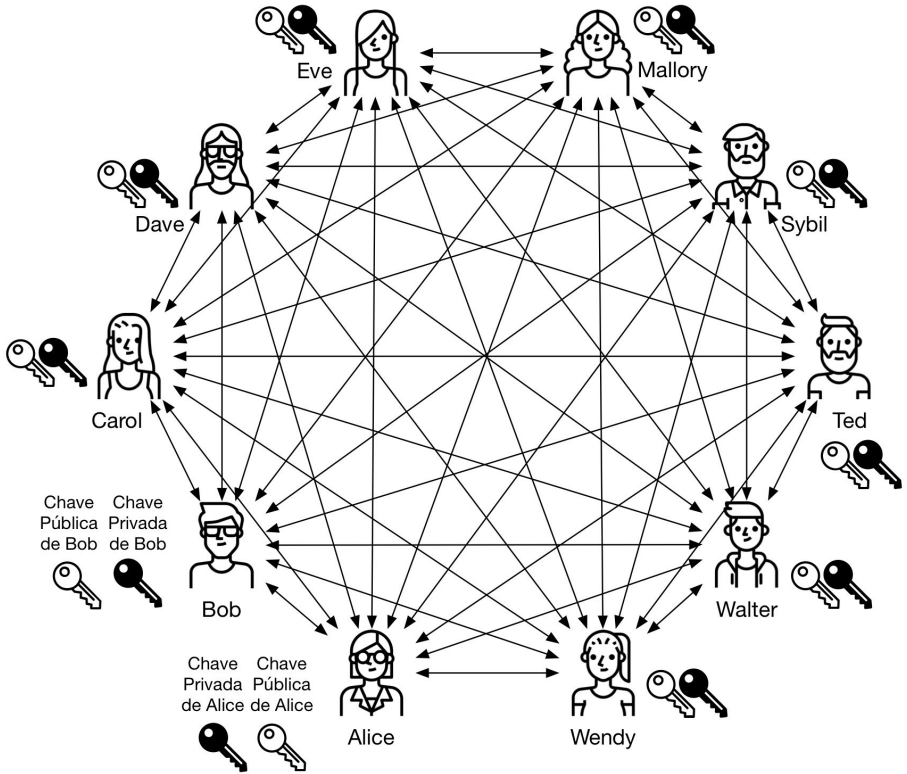
Par de Chaves Criptográficas



Par de Chaves Criptográficas



Par de Chaves Criptográficas

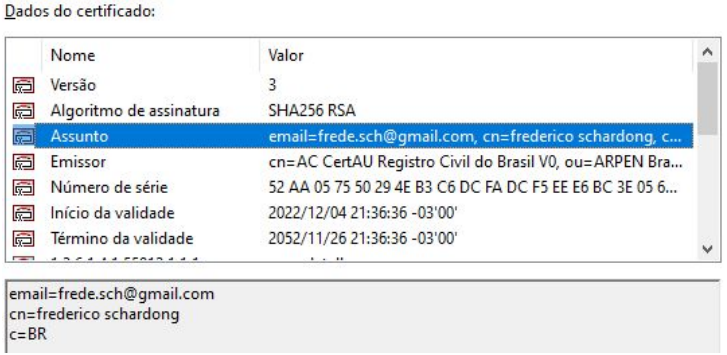


Certificado Digital

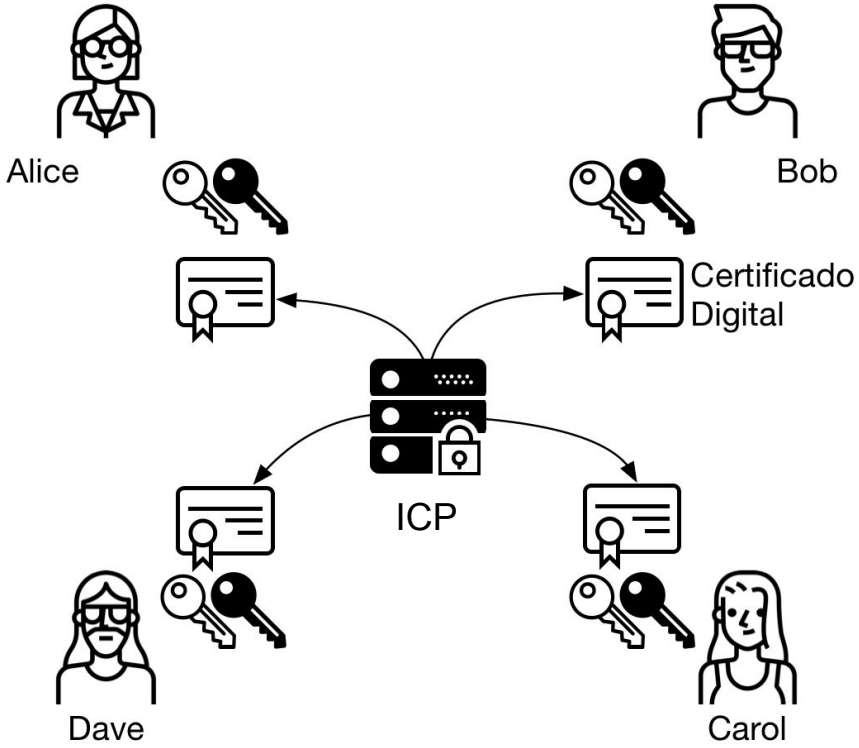
- Como descobrir a quem pertence uma chave pública?
- Em quem devemos confiar?

Certificado Digital

- Certificados Digitais ligam informações a uma chave pública



Infraestrutura de Chaves Públicas

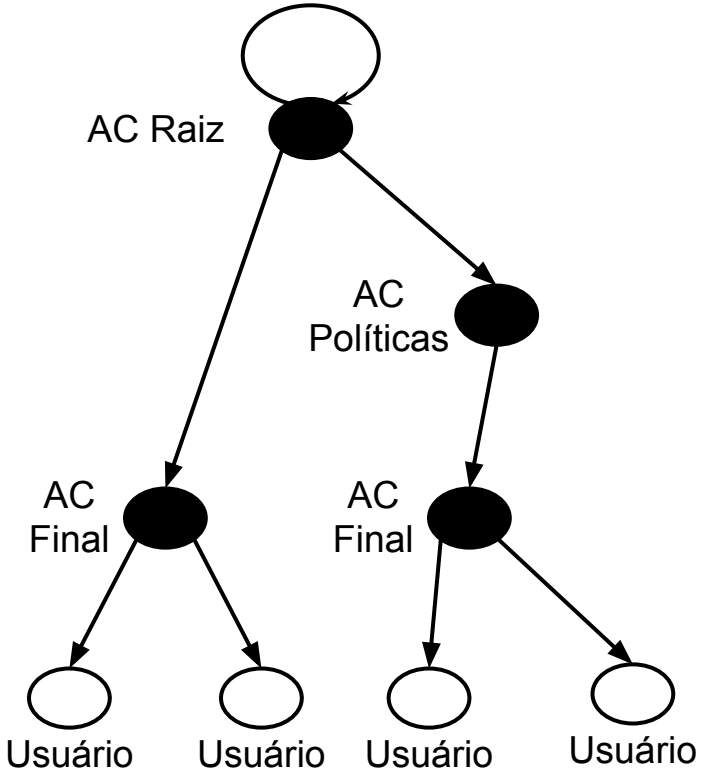


Infraestrutura de Chaves Públicas

ICP

É um conjunto de ferramentas, apoiadas por processos, que fornece serviços para a gestão segura e eficiente de chaves criptográficas.

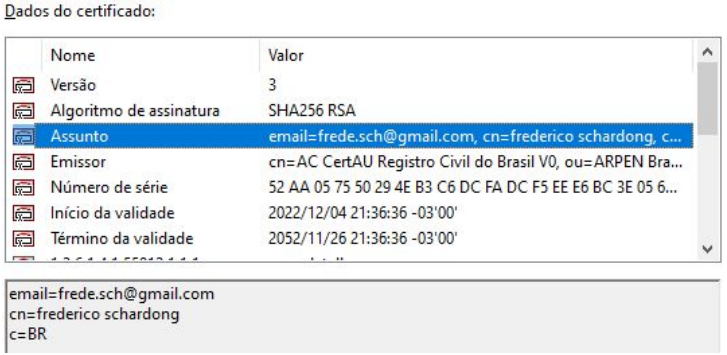
ICP - Árvore de Certificação

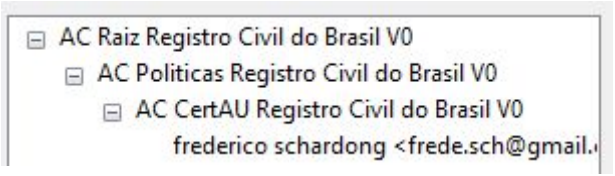


ICP - Árvore de Certificação

- Certificados Digitais ligam informações a uma chave pública

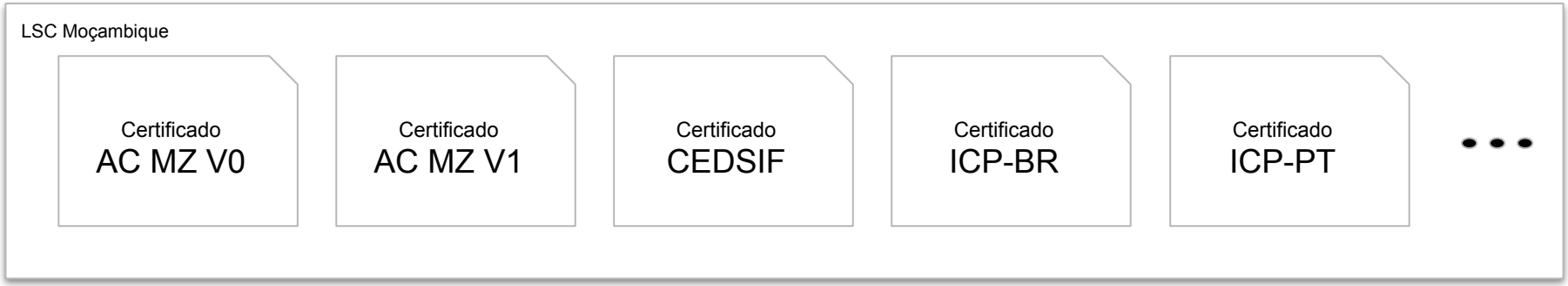
- Se confiamos no emissor, confiamos no certificado



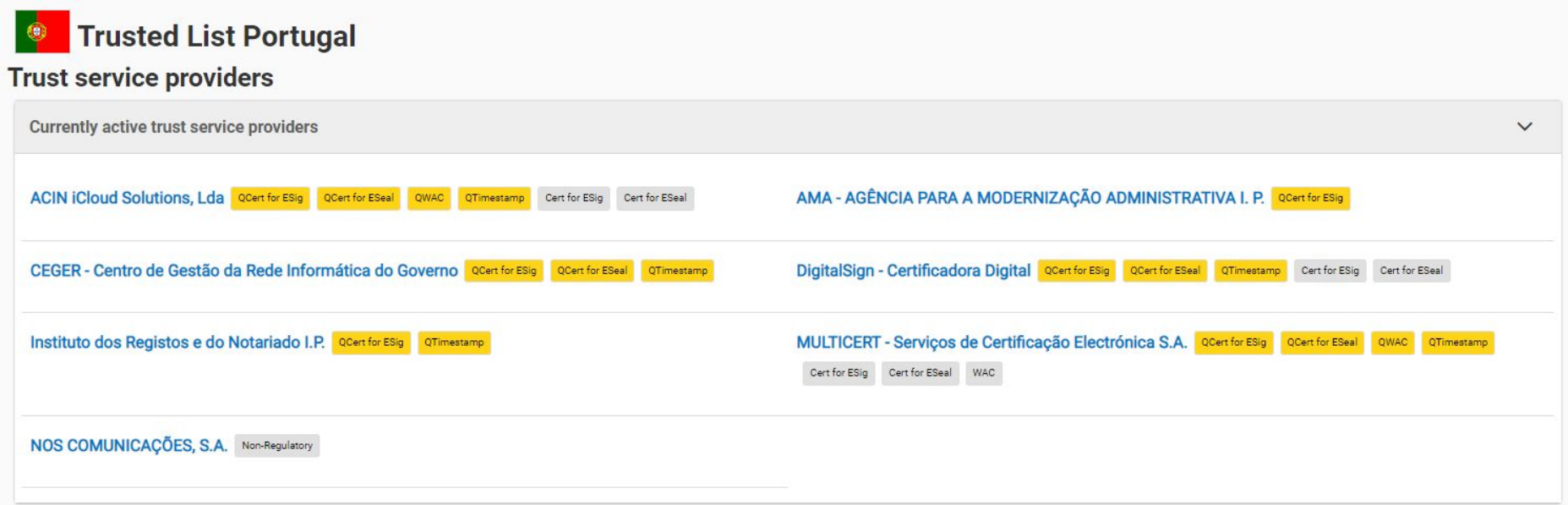


Lista de Serviços Confiáveis (LSC)

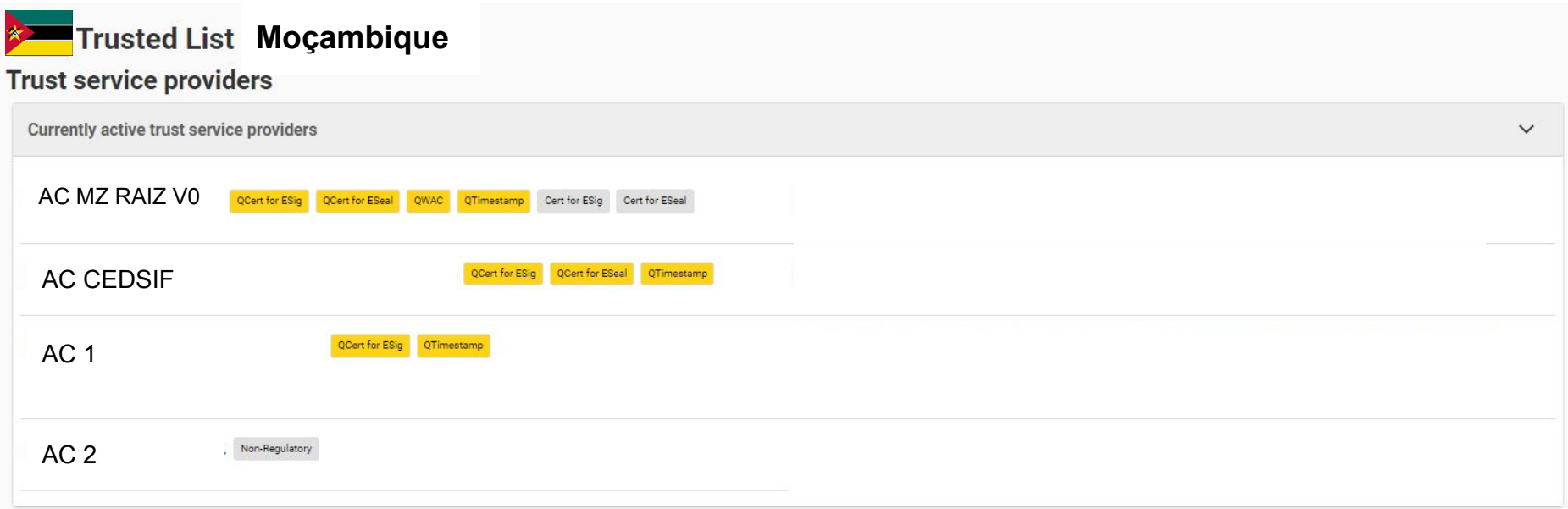
- Lista contendo os serviços de confiança
- Serviços podem ser adicionados/removidos sob demanda
- XML contendo informações sobre o serviço e seu certificado
- Poder fica na mão da entidade que publica a lista



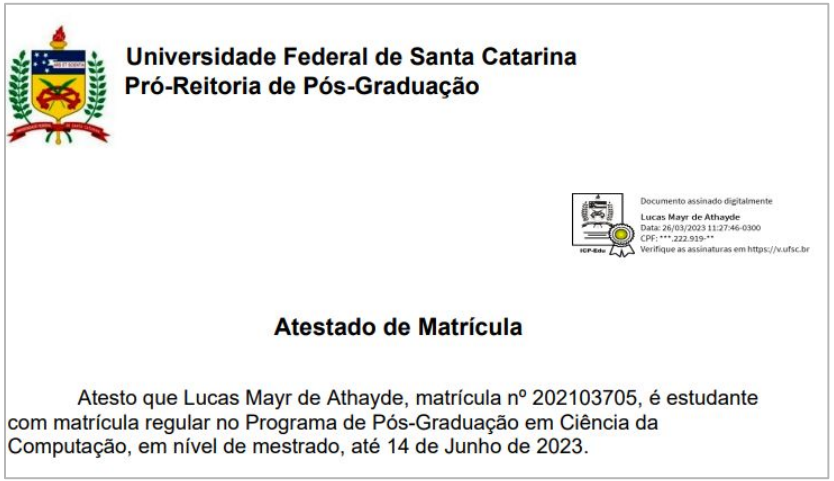
Lista de Serviços Confiáveis (LSC) - Portugal



Lista de Serviços Confiáveis (LSC) - Moçambique



Assinatura Digital

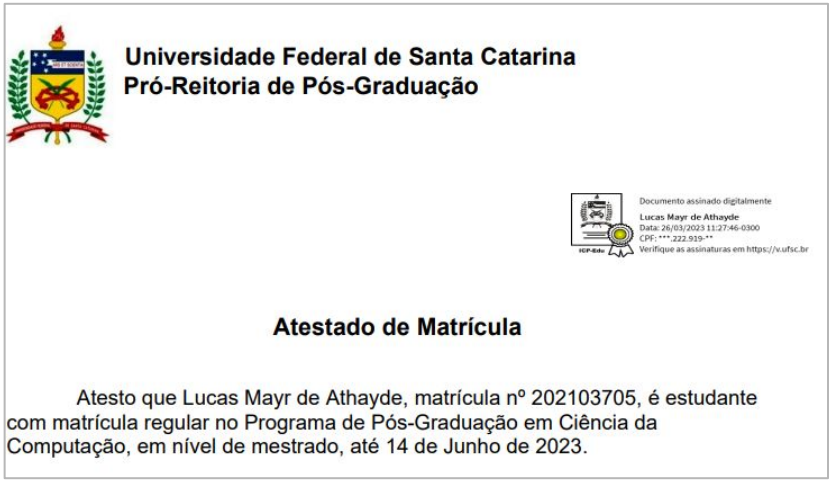


Universidade Federal de Santa Catarina
Pró-Reitoria de Pós-Graduação

Documento assinado digitalmente
Lucas Mayr de Athayde
Data: 26/03/2023 11:27:46-0300
CPF: ***.222.919-**
Verifique as assinaturas em https://v.ufsc.br

Atestado de Matrícula

Atesto que Lucas Mayr de Athayde, matrícula nº 202103705, é estudante com matrícula regular no Programa de Pós-Graduação em Ciência da Computação, em nível de mestrado, até 14 de Junho de 2023.



Universidade Federal de Santa Catarina
Pró-Reitoria de Pós-Graduação

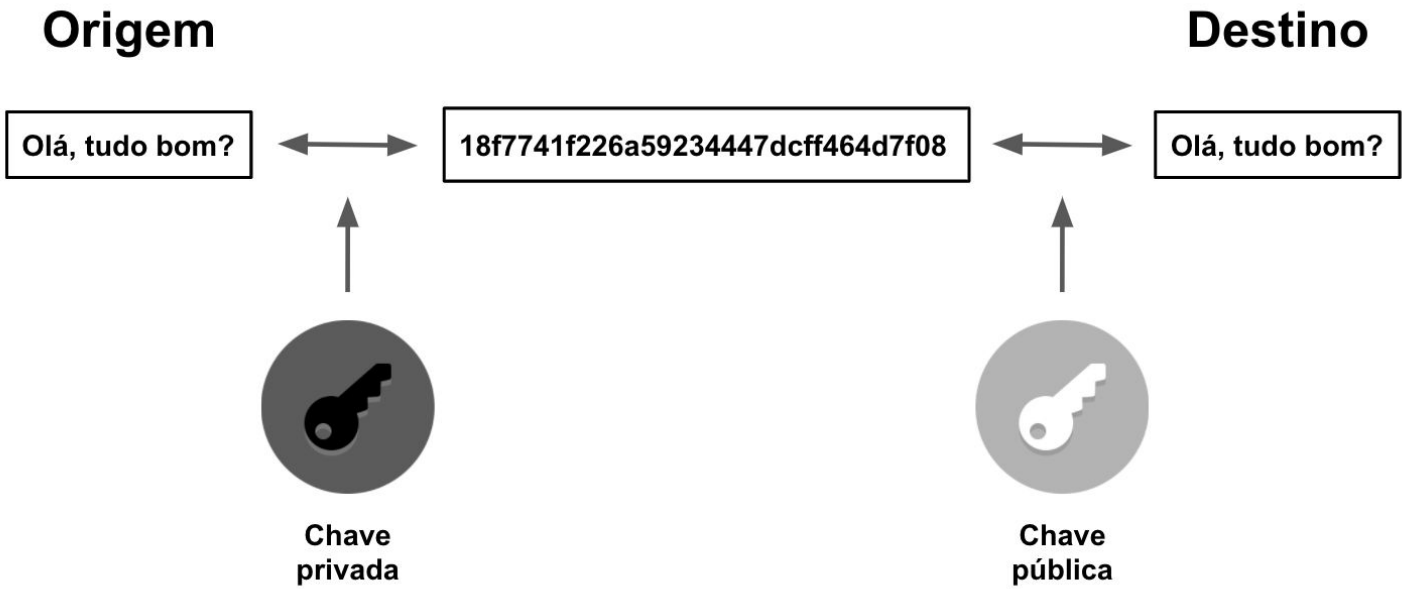
Documento assinado digitalmente
Lucas Mayr de Athayde
Data: 26/03/2023 11:27:46-0300
CPF: ***.222.919-**
Verifique as assinaturas em https://v.ufsc.br

Atestado de Matrícula

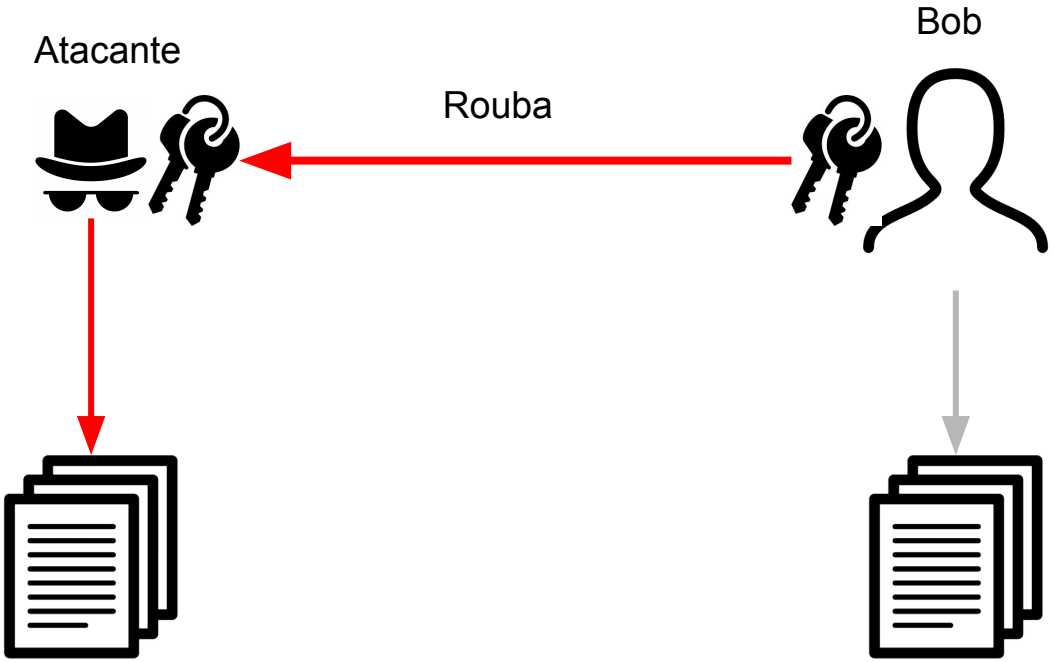
Atesto que Lucas Mayr de Athayde, matrícula nº 202103705, é estudante com matrícula regular no Programa de Pós-Graduação em Ciência da Computação, em nível de mestrado, até 14 de Junho de 2023.

Assinatura Digital

Chaves Privadas



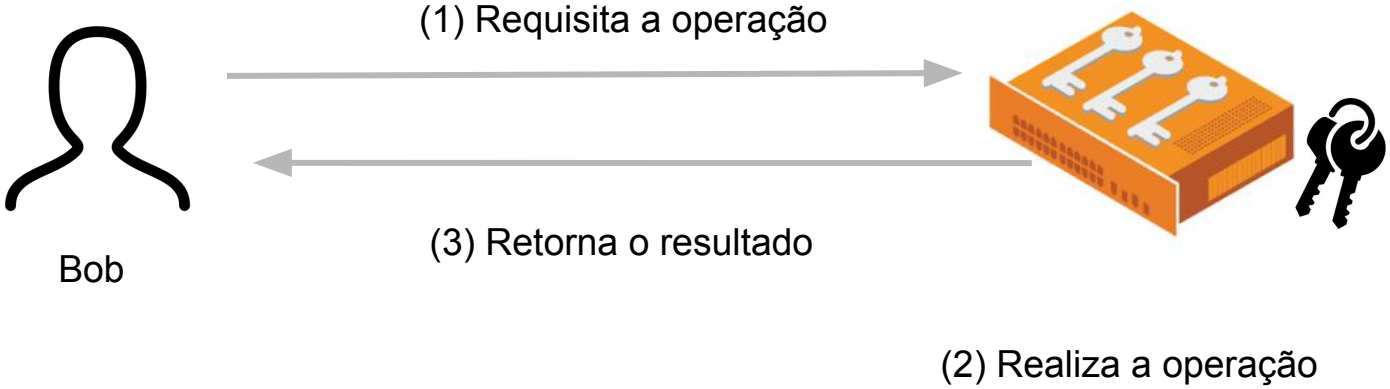
Chaves Privadas



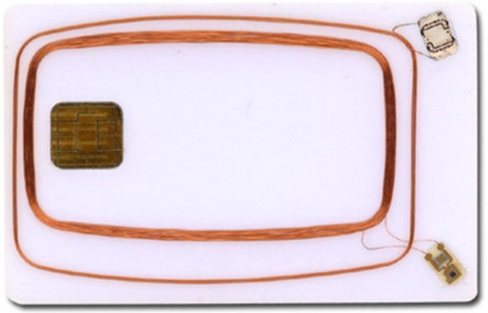
Métodos de Segurança - HSM

- Módulo de Segurança Criptográfico
- Tamper-resistance
- Tamper-proof
- Auditoria
- Registro de acesso
- Armazenamento seguro

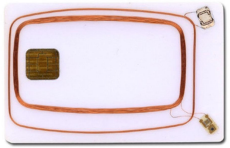
Métodos de Segurança - HSM



Métodos de Segurança - Smart Card

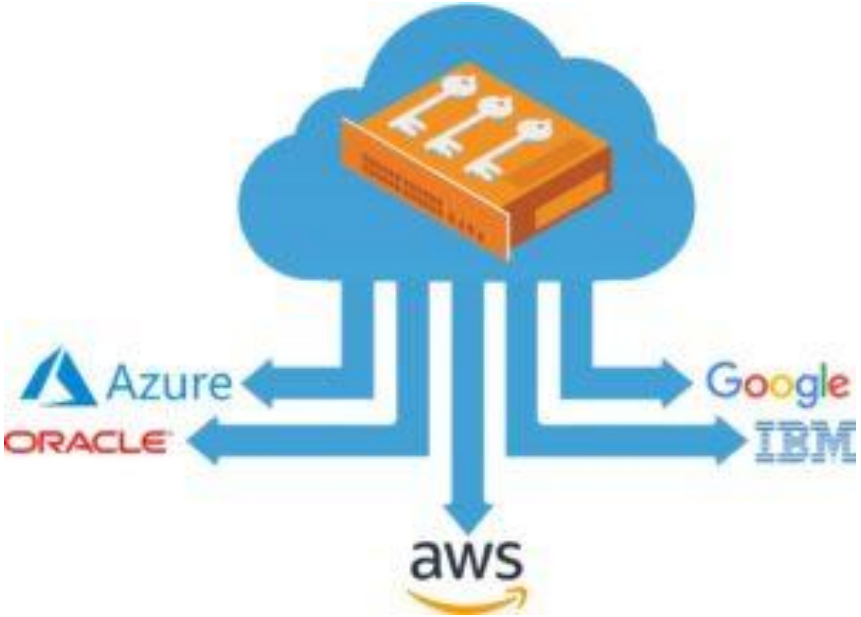


Métodos de Segurança - Tokens



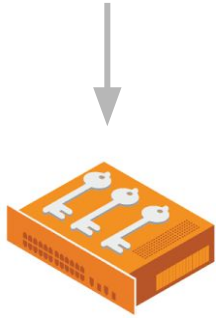
Métodos de Segurança - Cloud

Métodos de Segurança - Cloud

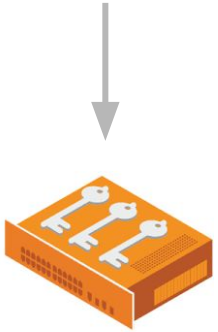


Onde Estão?

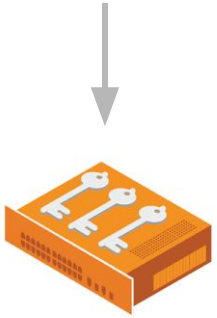
AC Raiz



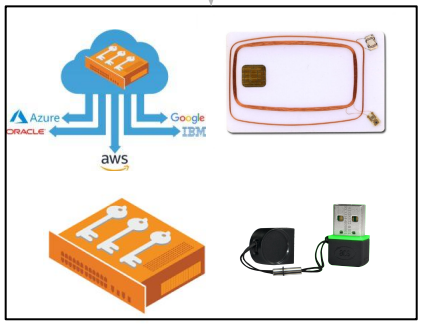
AC Intermediária



AC Final



Usuário

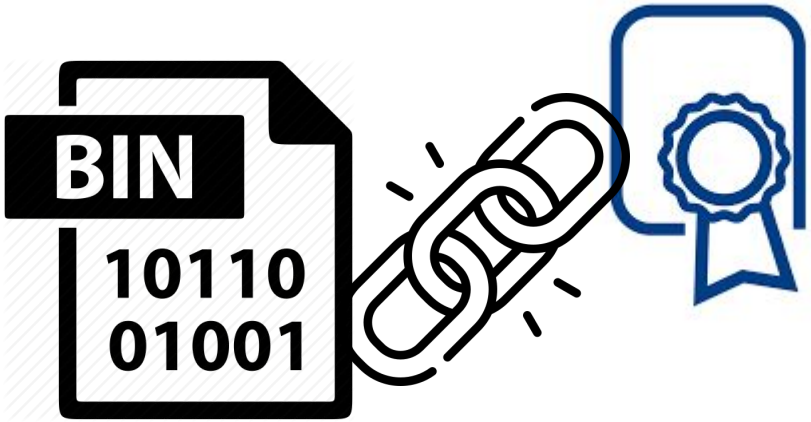


Certificado de Uso Único

1. Destruindo a chave privada após a assinatura;

Certificado de Uso Único

2. Limitando o certificado a **um** documento;



Obrigado

Perguntas?

Contato

lucas.mayr@posgrad.ufsc.br