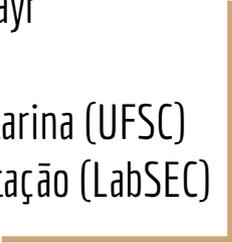




Introdução a Certificação Digital: Conceitos Básicos

Professor Bsc. Lucas Mayr

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

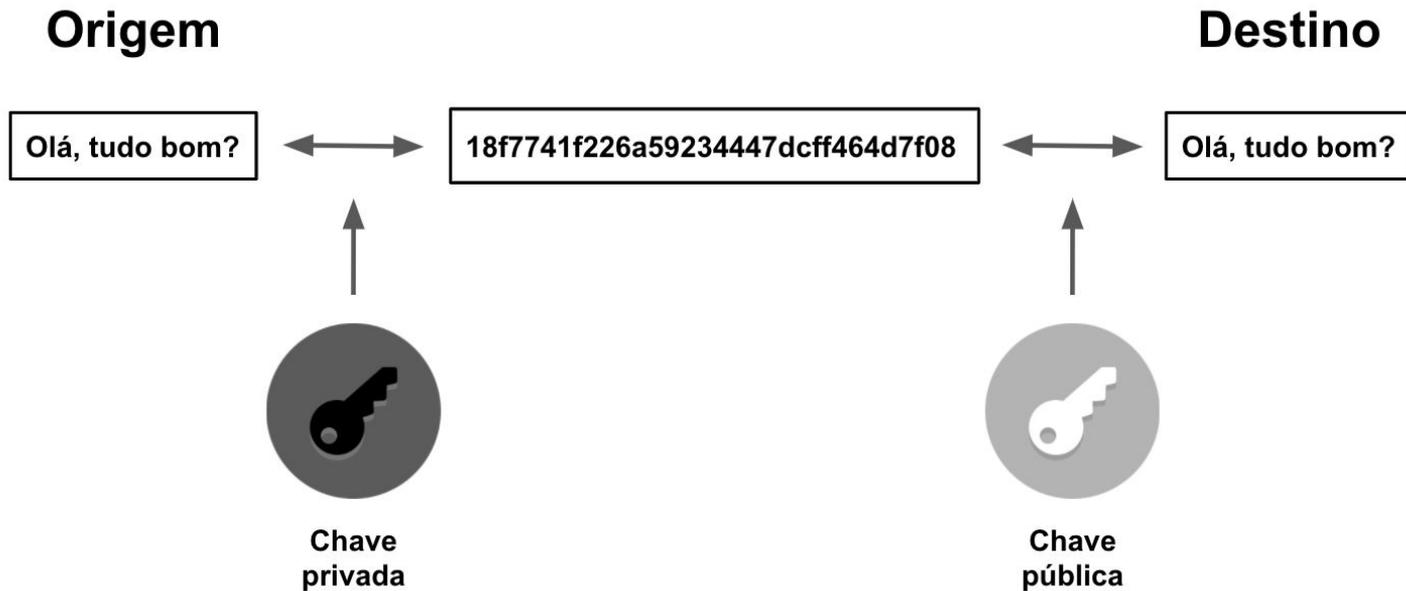


Março de 2023

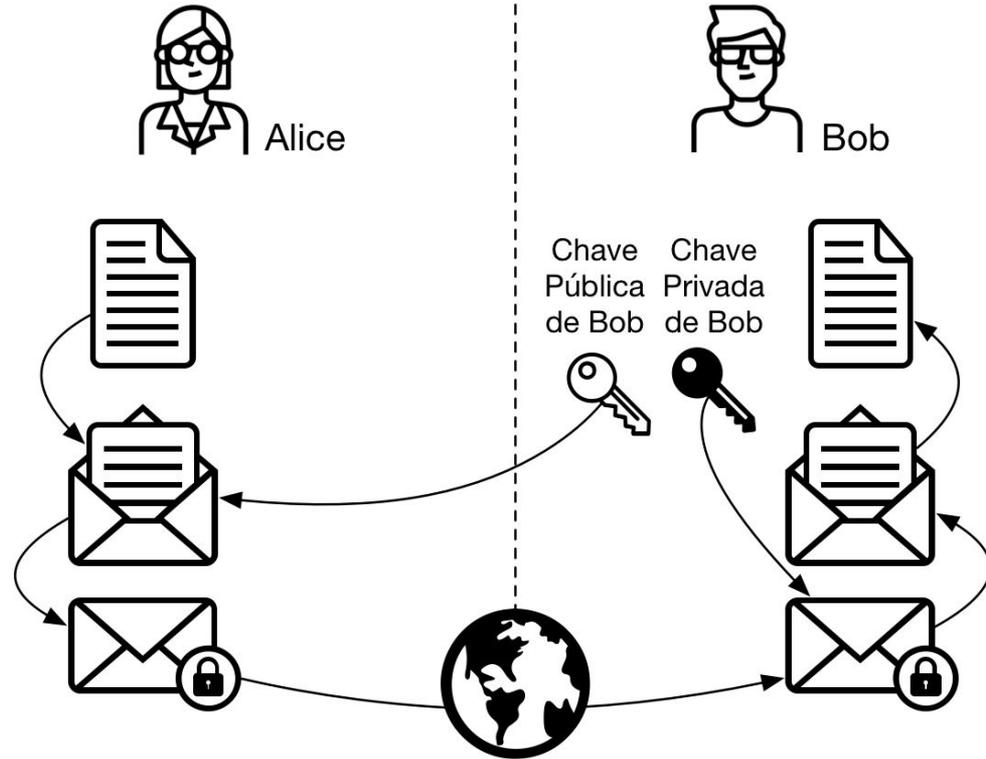
Documentos Electrónicos



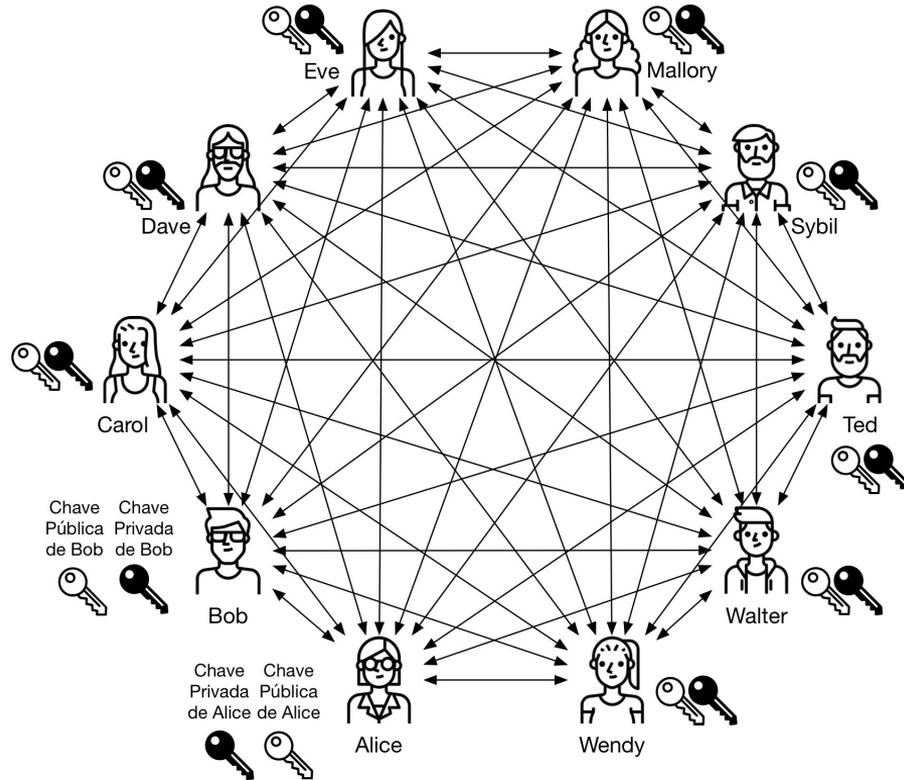
Par de Chaves Criptográficas



Par de Chaves Criptográficas



Par de Chaves Criptográficas



Certificado Digital

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

Certificado Digital

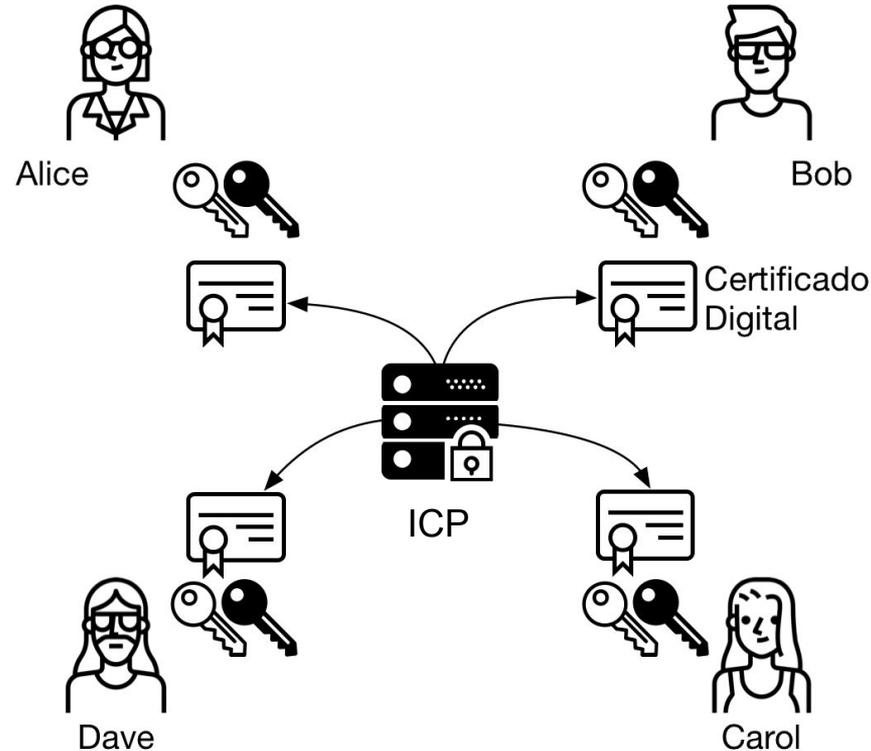
- Certificados Digitais ligam informações a uma chave pública

Dados do certificado:

Nome	Valor
Versão	3
Algoritmo de assinatura	SHA256 RSA
Assunto	email=frede.sch@gmail.com, cn=frederico schardong, c...
Emissor	cn=AC CertAU Registro Civil do Brasil V0, ou=ARPEN Bra...
Número de série	52 AA 05 75 50 29 4E B3 C6 DC FA DC F5 EE E6 BC 3E 05 6...
Início da validade	2022/12/04 21:36:36 -03'00'
Término da validade	2052/11/26 21:36:36 -03'00'

email=frede.sch@gmail.com
cn=frederico schardong
c=BR

Infraestrutura de Chaves Públicas

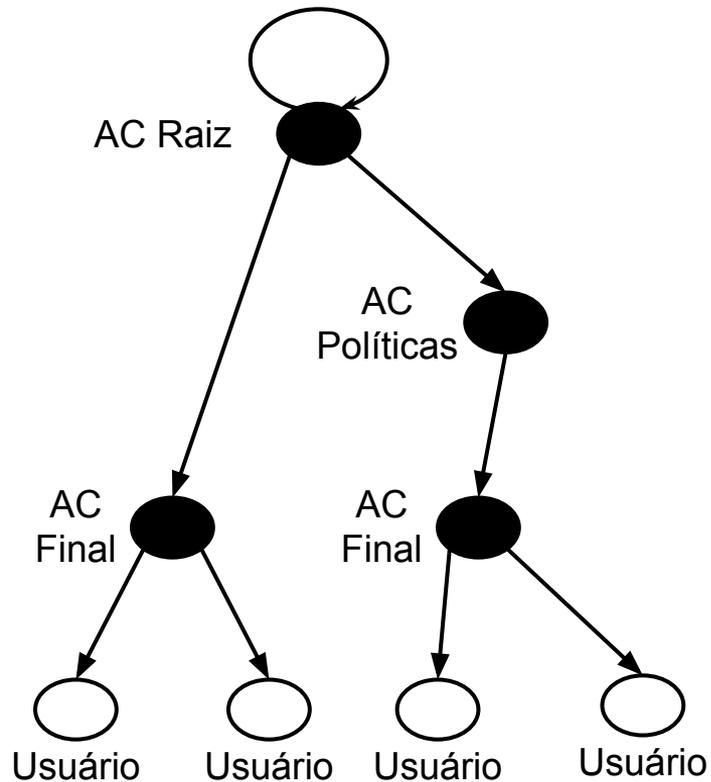


Infraestrutura de Chaves Públicas

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

Dados do certificado:

Nome	Valor
Versão	3
Algoritmo de assinatura	SHA256 RSA
Assunto	email=frede.sch@gmail.com, cn=frederico schardong, c...
Emissor	cn=AC CertAU Registro Civil do Brasil V0, ou=ARPEN Bra...
Número de série	52 AA 05 75 50 29 4E B3 C6 DC FA DC F5 EE E6 BC 3E 05 6...
Início da validade	2022/12/04 21:36:36 -03'00'
Término da validade	2052/11/26 21:36:36 -03'00'

email=frede.sch@gmail.com
cn=frederico schardong
c=BR

[-] AC Raiz Registro Civil do Brasil V0
[-] AC Políticas Registro Civil do Brasil V0
[-] AC CertAU Registro Civil do Brasil V0
frederico schardong <frede.sch@gmail.com>

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



Trusted List Portugal

Trust service providers

Currently active trust service providers



[ACIN iCloud Solutions, Lda](#) QCert for ESig QCert for ESeal QWAC QTimestamp Cert for ESig Cert for ESeal

[AMA - AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA I. P.](#) QCert for ESig

[CEGER - Centro de Gestão da Rede Informática do Governo](#) QCert for ESig QCert for ESeal QTimestamp

[DigitalSign - Certificadora Digital](#) QCert for ESig QCert for ESeal QTimestamp Cert for ESig Cert for ESeal

[Instituto dos Registos e do Notariado I.P.](#) QCert for ESig QTimestamp

[MULTICERT - Serviços de Certificação Electrónica S.A.](#) QCert for ESig QCert for ESeal QWAC QTimestamp

Cert for ESig Cert for ESeal WAC

[NOS COMUNICAÇÕES, S.A.](#) Non-Regulatory

Lista de Serviços Confiáveis (LSC) - Moçambique



Trusted List Moçambique

Trust service providers

Currently active trust service providers

AC MZ RAIZ V0

QCert for ESig

QCert for ESeal

QWAC

QTimestamp

Cert for ESig

Cert for ESeal

AC CEDSIF

QCert for ESig

QCert for ESeal

QTimestamp

AC 1

QCert for ESig

QTimestamp

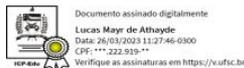
AC 2

Non-Regulatory

Assinatura Digital



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

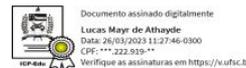


Atestado de Matrícula

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**



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

✓ **Sucesso!**

Todas as assinaturas do documento estão válidas

Assinado digitalmente por:



Lucas Mayr de Athayde em 26/03/2023 11:27:46

Documento não foi modificado após a assinatura.

Cadeia de certificação da assinatura é reconhecida.

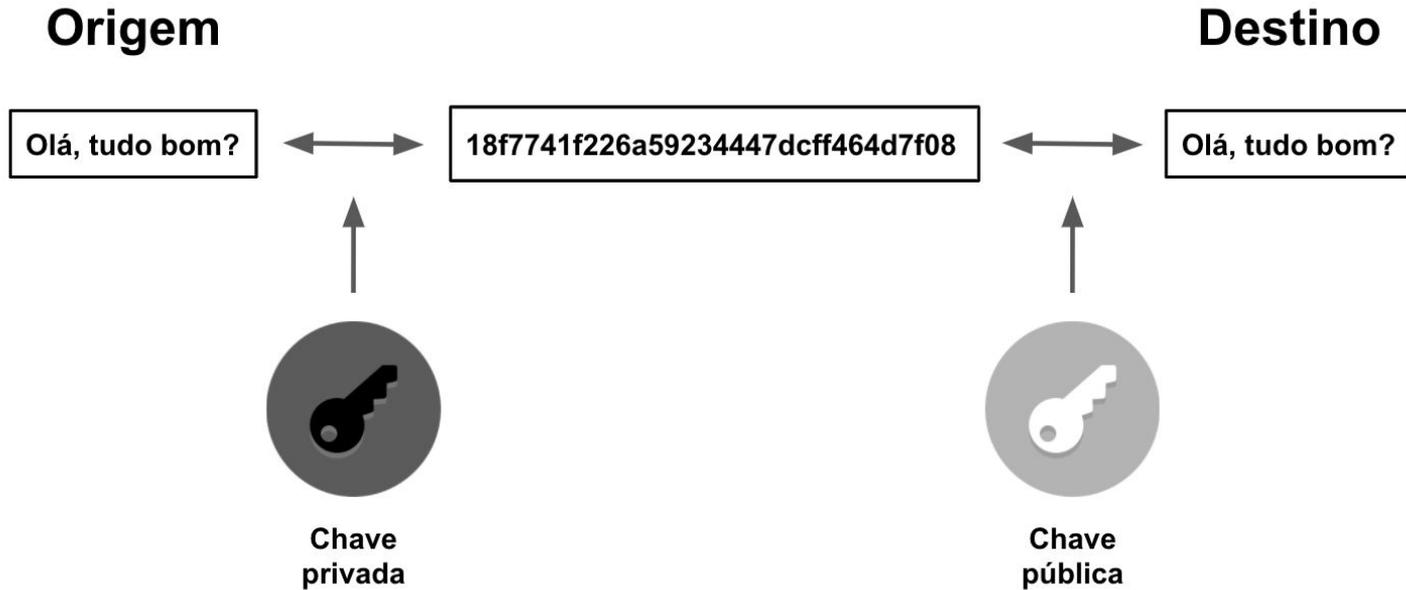
A assinatura possui um carimbo de tempo incorporado.

Assinatura com certificado ICP-Edu

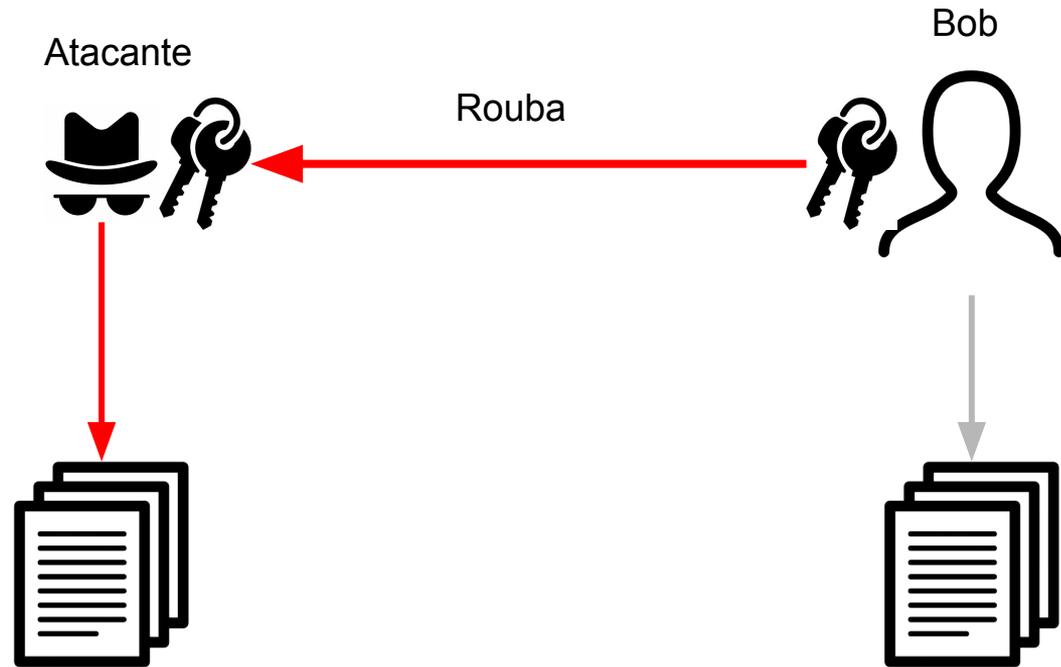
⚠ **Atenção!**

Não foi possível encontrar assinaturas digitais no documento selecionado

Chaves Privadas



Chaves Privadas

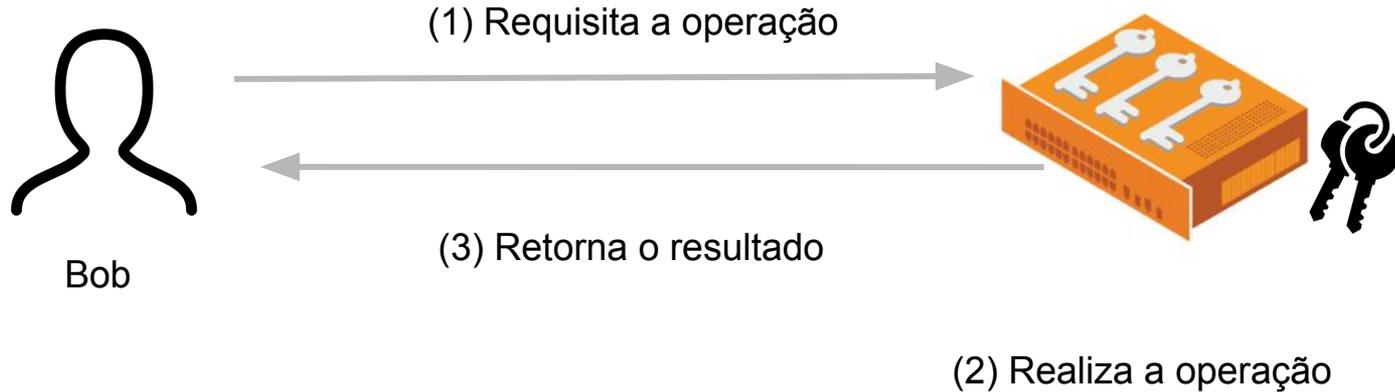


Métodos de Segurança - HSM

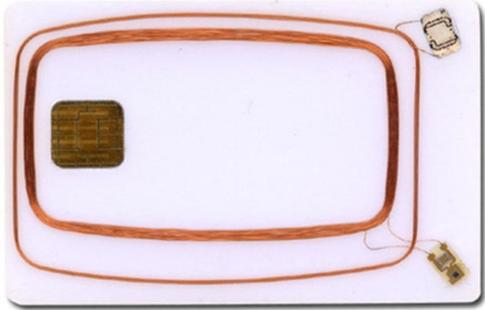
- Módulo de Segurança Criptográfico
- Tamper-resistance
- Tamper-proof
- Auditoria
- Registro de acesso
- Armazenamento seguro



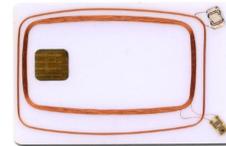
Métodos de Segurança - HSM



Métodos de Segurança - Smart Card



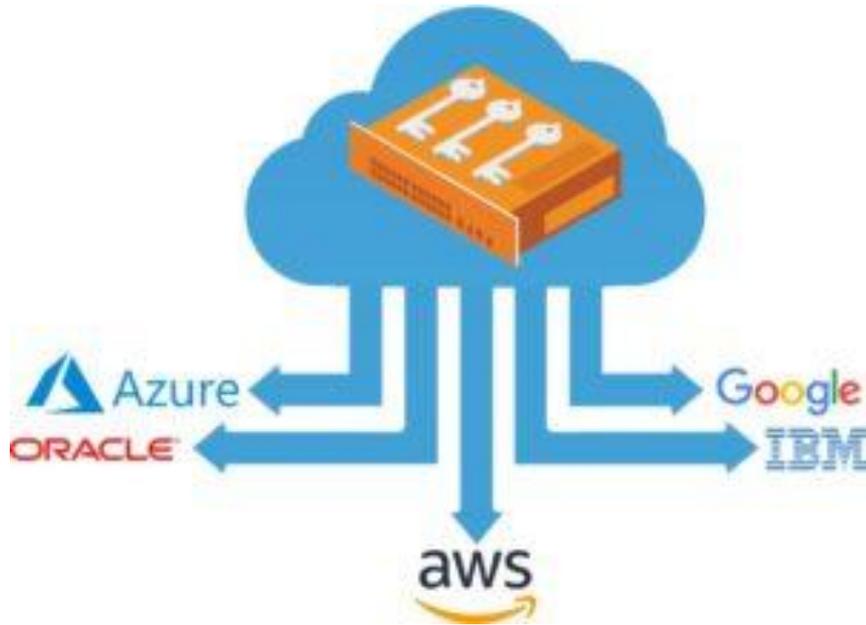
Métodos de Segurança - Tokens



Métodos de Segurança - Cloud



Métodos de Segurança - Cloud



Onde Estão?

AC Raiz



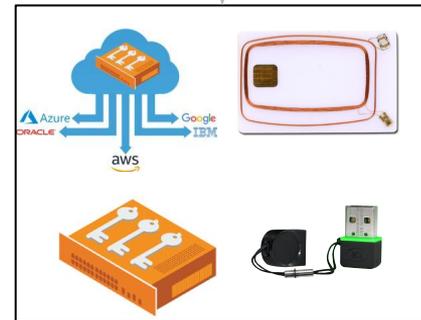
AC Intermediária



AC Final



Usuário



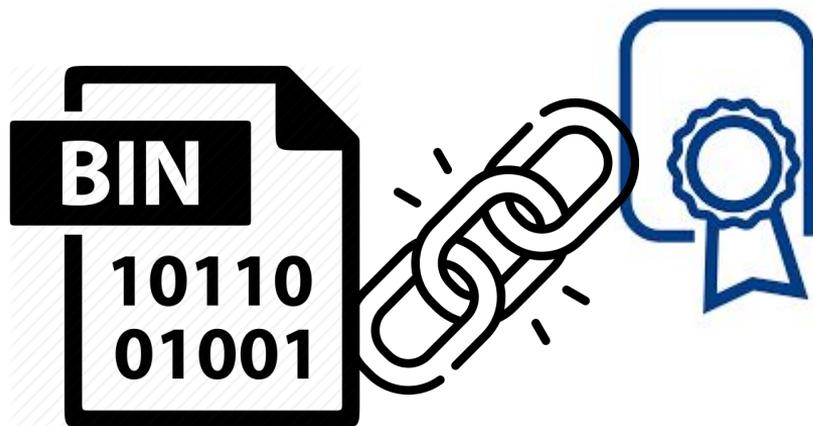
Certificado de Uso Único

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