

Certificado digital e assinatura eletrônica

SEG786203 – CST em Análise e Desenvolvimento de Sistemas

Prof. Emerson Ribeiro de Mello

mello@ifsc.edu.br

Licenciamento



Slides licenciados sob [Creative Commons “Atribuição 4.0 Internacional”](#)

Sumário

1 Introdução

2 Certificado digital

3 Assinatura eletrônica

Introdução

Objetivos dessa aula

- Entender o que é um certificado digital
- Entender o que é uma Infraestrutura de Chaves Públicas (ICP)
- Entender o que é uma assinatura eletrônica

Problemas

- 1 Baixar uma imagem ISO de um sistema operacional e ter certeza sobre a autenticidade e a integridade do arquivo
- 2 Acessar um site de comércio eletrônico e ter certeza de que o site é autêntico
- 3 Verificar se um atestado de matrícula emitido por uma instituição de ensino é autêntico

Problemas

- 1 Baixar uma imagem ISO de um sistema operacional e ter certeza sobre a autenticidade e a integridade do arquivo
- 2 Acessar um site de comércio eletrônico e ter certeza de que o site é autêntico
- 3 Verificar se um atestado de matrícula emitido por uma instituição de ensino é autêntico

Exercício em duplas (10 minutos)

- Pense em possíveis soluções para os problemas acima
- Use o conhecimento que você já possui sobre tecnologias e ferramentas

Problemas

Discussão

- 1 Baixar uma imagem ISO de um sistema operacional e ter certeza sobre a autenticidade e a integridade do arquivo**
 - Criptografia de chave pública ajuda, mas como garantir que a chave pública é autêntica?
- 2 Acessar um site de comércio eletrônico e ter certeza de que o site é autêntico**
 - O site usa HTTPS, mas como garantir que o certificado digital é autêntico?
- 3 Verificar se um atestado de matrícula emitido por uma instituição de ensino é autêntico**
 - O documento tem uma assinatura eletrônica, mas como garantir que a assinatura é autêntica?

Certificado digital

Assinatura digital com criptografia assimétrica

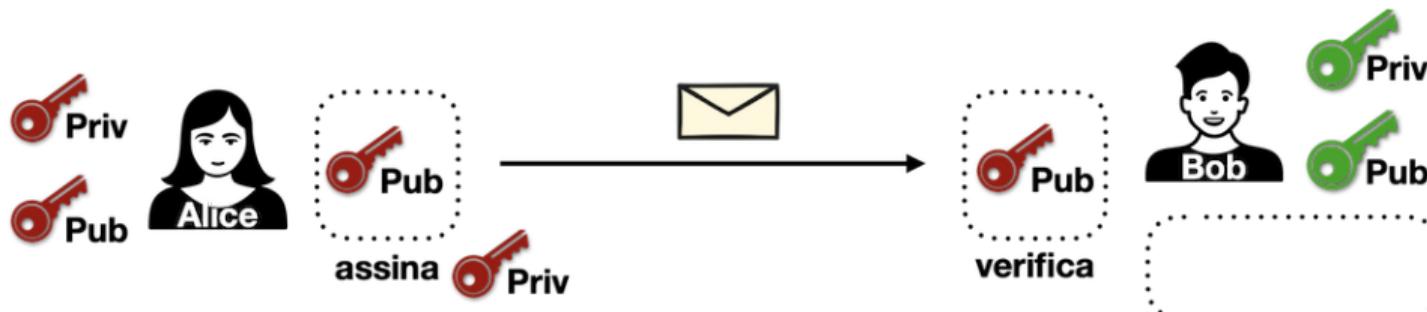
Se a assinatura for válida...

- **É possível ter certeza** que alguém, com acesso à chave privada, assinou a mensagem
- **Não é possível afirmar** que a assinatura foi feita por uma pessoa específica (e.g. Alice)

Assinatura digital com criptografia assimétrica

Se a assinatura for válida...

- É possível ter certeza que alguém, com acesso à chave privada, assinou a mensagem
- Não é possível afirmar que a assinatura foi feita por uma pessoa específica (e.g. Alice)

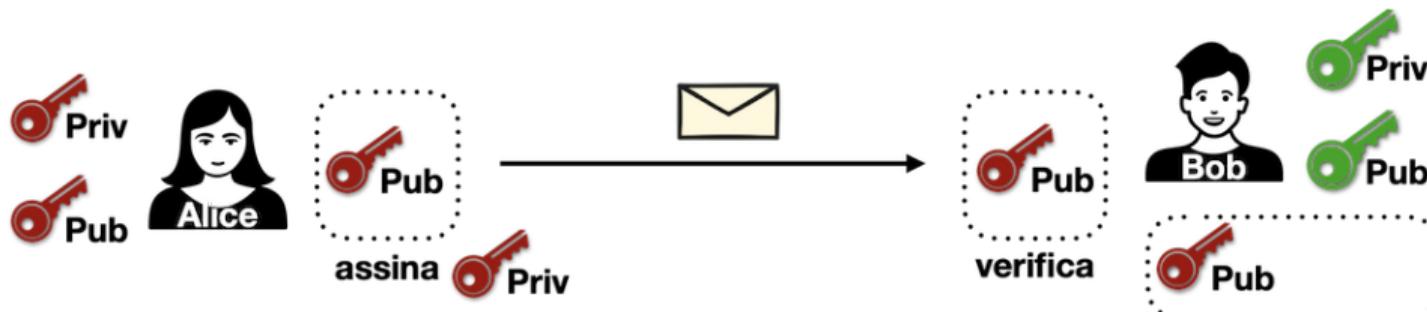


Troca de chaves públicas entre Alice e Bob

Assinatura digital com criptografia assimétrica

Se a assinatura for válida...

- É possível ter certeza que alguém, com acesso à chave privada, assinou a mensagem
- Não é possível afirmar que a assinatura foi feita por uma pessoa específica (e.g. Alice)

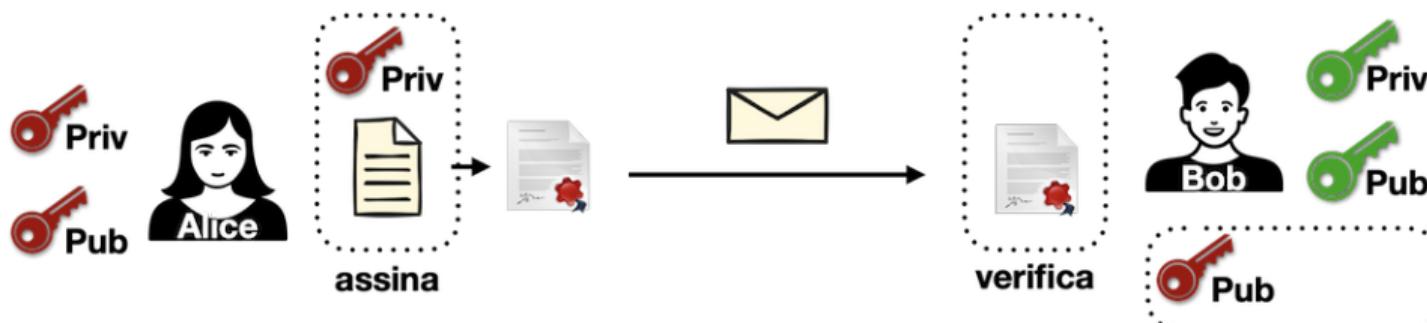


Troca de chaves públicas entre Alice e Bob

Assinatura digital com criptografia assimétrica

Se a assinatura for válida...

- É possível ter certeza que alguém, com acesso à chave privada, assinou a mensagem
- Não é possível afirmar que a assinatura foi feita por uma pessoa específica (e.g. Alice)

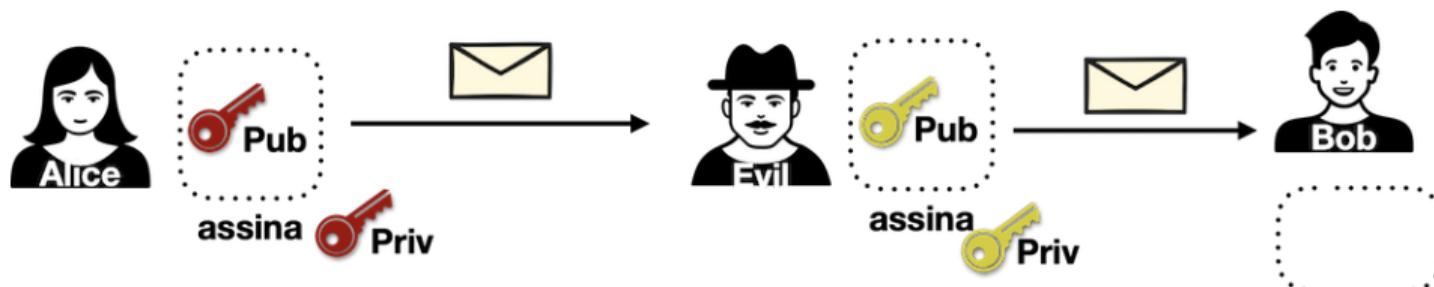


Troca de chaves públicas entre Alice e Bob

Assinatura digital com criptografia assimétrica

Se a assinatura for válida...

- É possível ter certeza que alguém, com acesso à chave privada, assinou a mensagem
- Não é possível afirmar que a assinatura foi feita por uma pessoa específica (e.g. Alice)

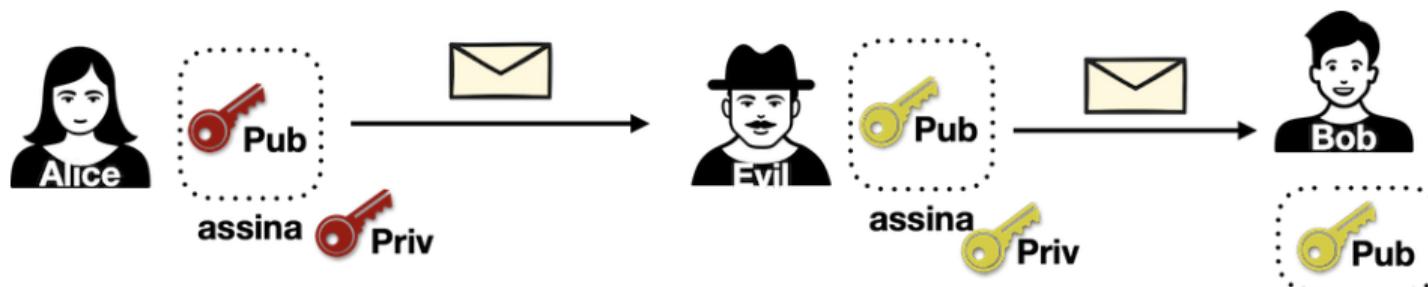


Ataque do homem no meio (MITM, *Main-in-the-middle*)

Assinatura digital com criptografia assimétrica

Se a assinatura for válida...

- É possível ter certeza que alguém, com acesso à chave privada, assinou a mensagem
- Não é possível afirmar que a assinatura foi feita por uma pessoa específica (e.g. Alice)

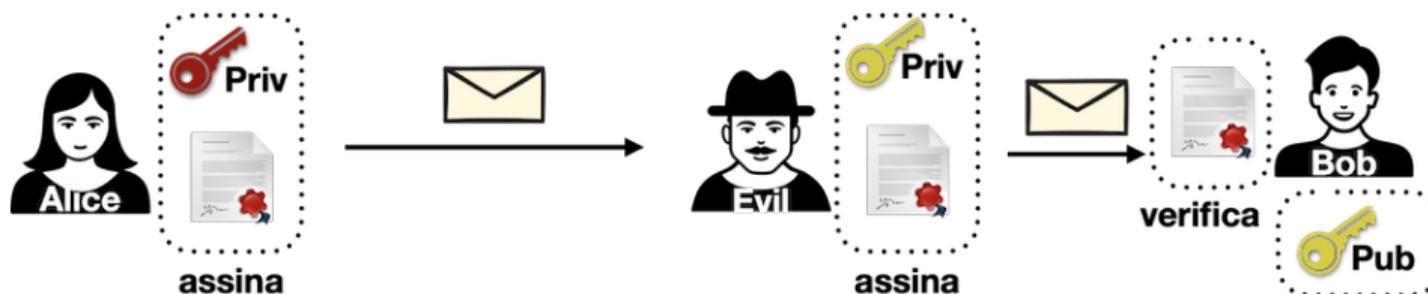


Ataque do homem no meio (MITM, *Main-in-the-middle*)

Assinatura digital com criptografia assimétrica

Se a assinatura for válida...

- É possível ter certeza que alguém, com acesso à chave privada, assinou a mensagem
- Não é possível afirmar que a assinatura foi feita por uma pessoa específica (e.g. Alice)



Ataque do homem no meio (MITM, *Main-in-the-middle*)

Assinatura digital com criptografia assimétrica

Se a assinatura for válida...

- É possível ter certeza que alguém, com acesso à chave privada, assinou a mensagem
- Não é possível afirmar que a assinatura foi feita por uma pessoa específica (e.g. Alice)



Ataque do homem no meio (MITM, *Main-in-the-middle*)

Certificado digital

Certificado de chave pública ou certificado de identidade

- **Associa dados de uma entidade a uma chave pública**

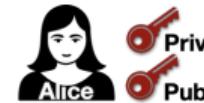
- Pessoa física, pessoa jurídica, servidor
- nome, e-mail, CPF, CNPJ etc

- **Confiança no emissor do certificado**

- Semelhante a confiança que você deposita em um cartório para reconhecer firma

- **Possuem validade e podem ser revogados**

- Não válido antes de uma data e não válido depois de uma data



Autoridade Certificadora (AC)

Entidade que emite certificados para servidores, pessoas físicas, pessoas jurídicas, etc

- Considerada como uma **Terceira parte confiável**
 - Duas partes que não confiam uma na outra confiam na AC
- A confiança na AC é baseada em
 - **Reputação** da AC
 - **Políticas** de emissão de certificados
 - **Procedimentos** de validação da identidade do solicitante
- **Navegadores e sistemas operacionais possuem uma lista de ACs confiáveis**
 - Certificados digitais emitidos por ACs confiáveis são aceitos sem alertas
 - Certificados digitais emitidos por ACs não confiáveis são rejeitados ou alertados

Autoridade Certificadora (AC)

Exemplos

■ Let's Encrypt

- Emite certificados digitais gratuitos para servidores HTTPS
- Certificados digitais com validade de 90 dias e renovados automaticamente
- Requer cliente ACME (*Automated Certificate Management Environment*) para automatizar a emissão e renovação

■ DigiCert, GoDaddy, GlobalSign, etc.

- Emite certificados digitais para servidores, pessoas físicas, pessoas jurídicas
- Certificados digitais com validade de 1 a 3 anos

Certificado digital para servidor web (certificado SSL/TLS)

Certificado no padrão X.509 v3

Certificate Viewer: *.ifsc.edu.br

General Details

Issued To

Common Name (CN)	*.ifsc.edu.br
Organization (O)	INSTITUTO FEDERAL DE EDUCACAO, CIENCIA E TECNOLOGIA DE SC
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	RNP ICP-Edu OV SSL CA 2019
Organization (O)	Rede Nacional de Ensino e Pesquisa - RNP
Organizational Unit (OU)	<Not Part Of Certificate>

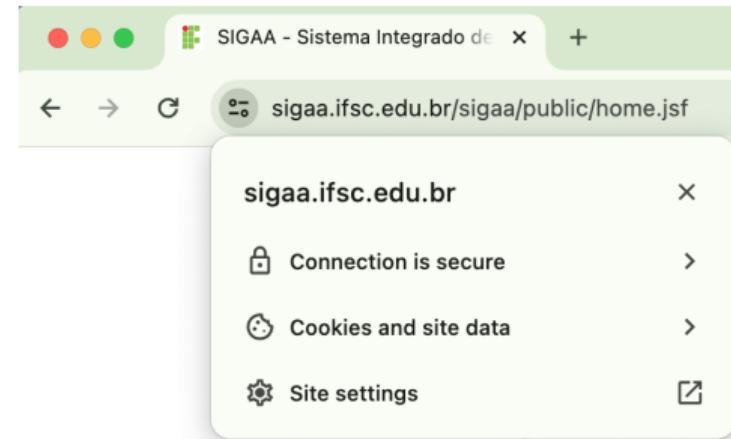
Validity Period

Issued On	Monday, August 7, 2023 at 4:26:09 PM
Expires On	Saturday, September 7, 2024 at 4:26:08 PM

SHA-256 Fingerprints

Certificate	3ba47b524ef29b7711e460257c184625e571b674a0ec9764820f aac48149edd4
Public Key	f39b17b1dd8f2bbd986a15807bce6d20294e01ee17d590a6597e 5cff2d3b8712

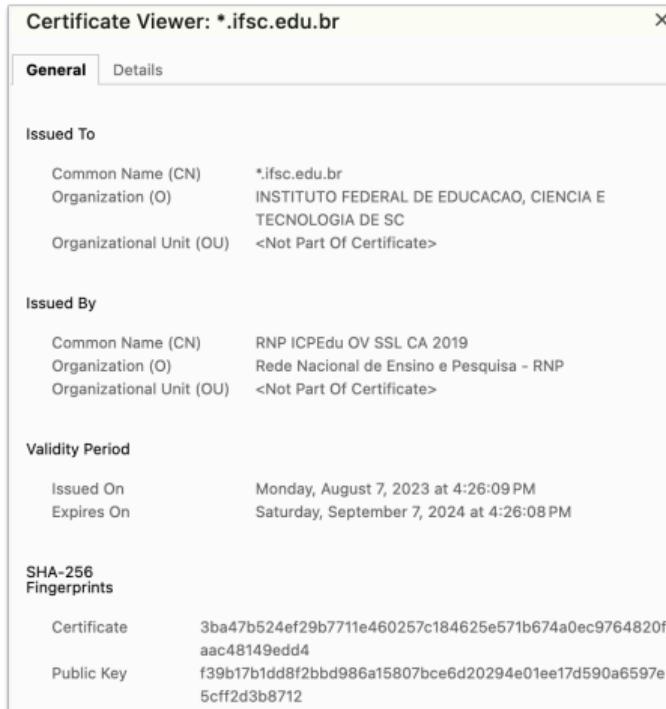
Certificado digital emitido para o IFSC



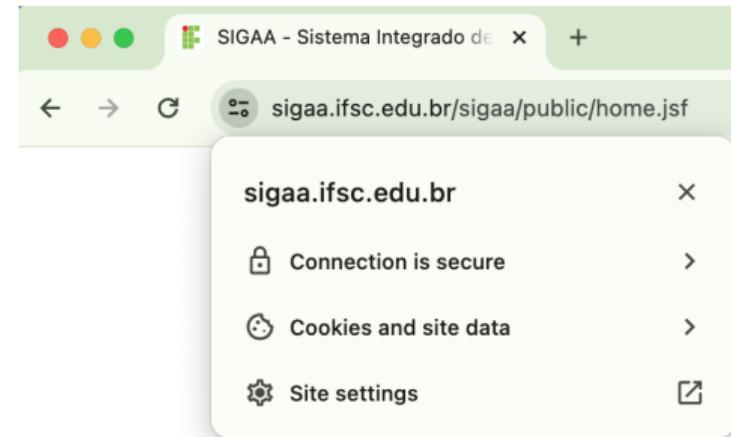
- Como o navegador determina que certificado é confiável?

Certificado digital para servidor web (certificado SSL/TLS)

Certificado no padrão X.509 v3



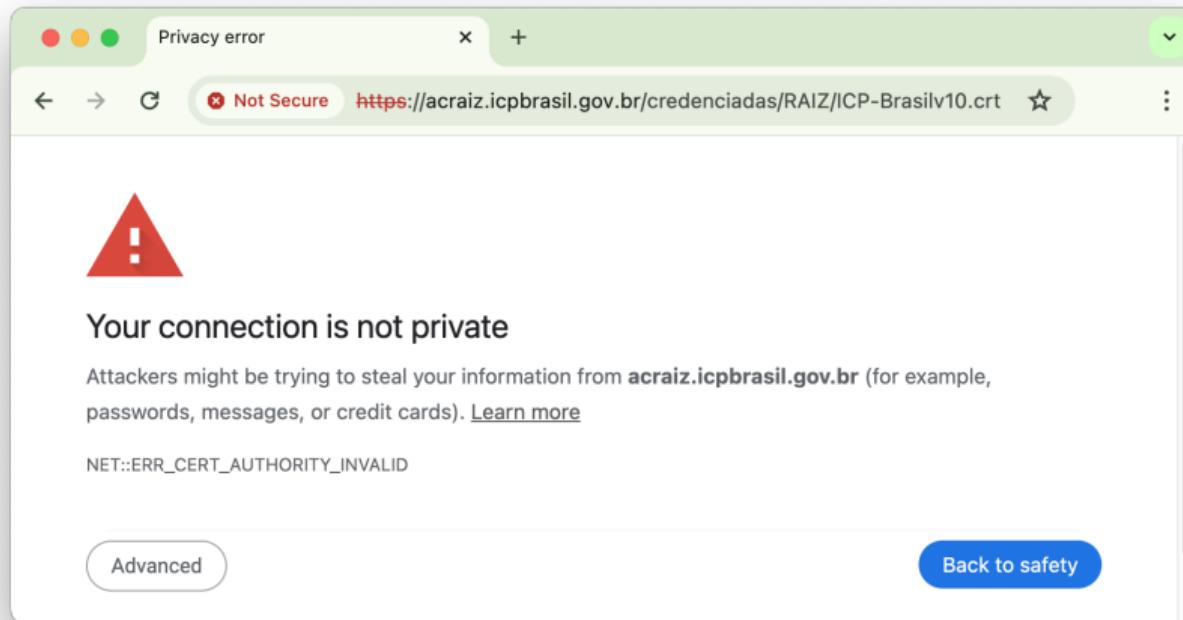
Certificado digital emitido para o IFSC



- Como o navegador determina que certificado é confiável?
 - Mantém uma lista de Autoridades Certificadoras (AC) confiáveis (âncoras de confiança)

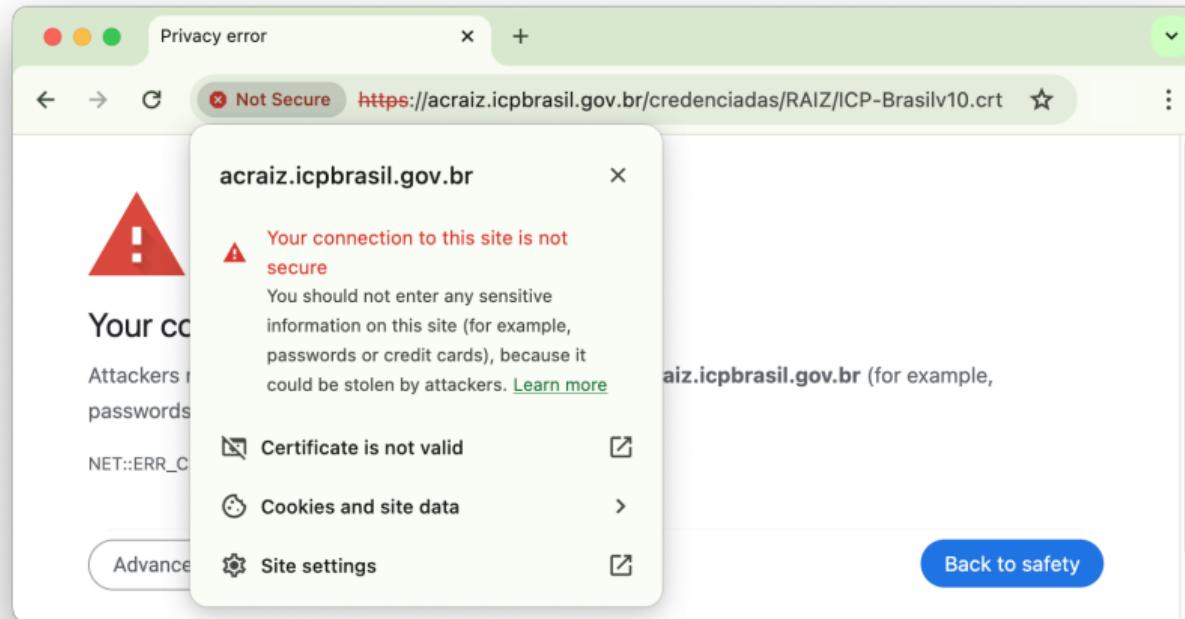
Certificado digital para servidor web

Navegador web não confia no emissor do certificado



Certificado digital para servidor web

Navegador web não confia no emissor do certificado



Certificados autoassinados I

■ Usado para testes e desenvolvimento

- Rápido e fácil de configurar
- Nunca devem ser usados em produção

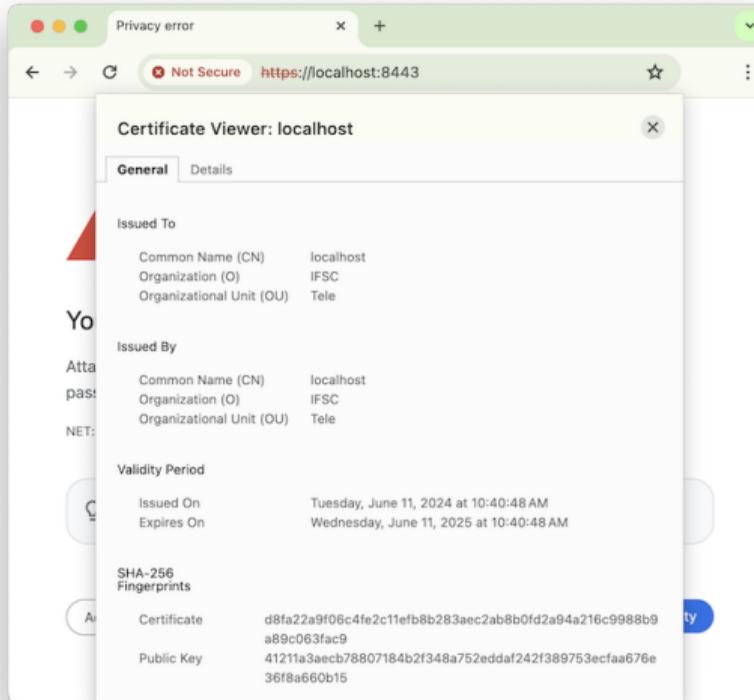
■ Emitido e assinado pela mesma entidade

- Navegadores e S.O. não confiam em certificados autoassinados
- O cliente é alertado que o certificado não é confiável

■ Permite a comunicação cifrada entre o cliente e o servidor

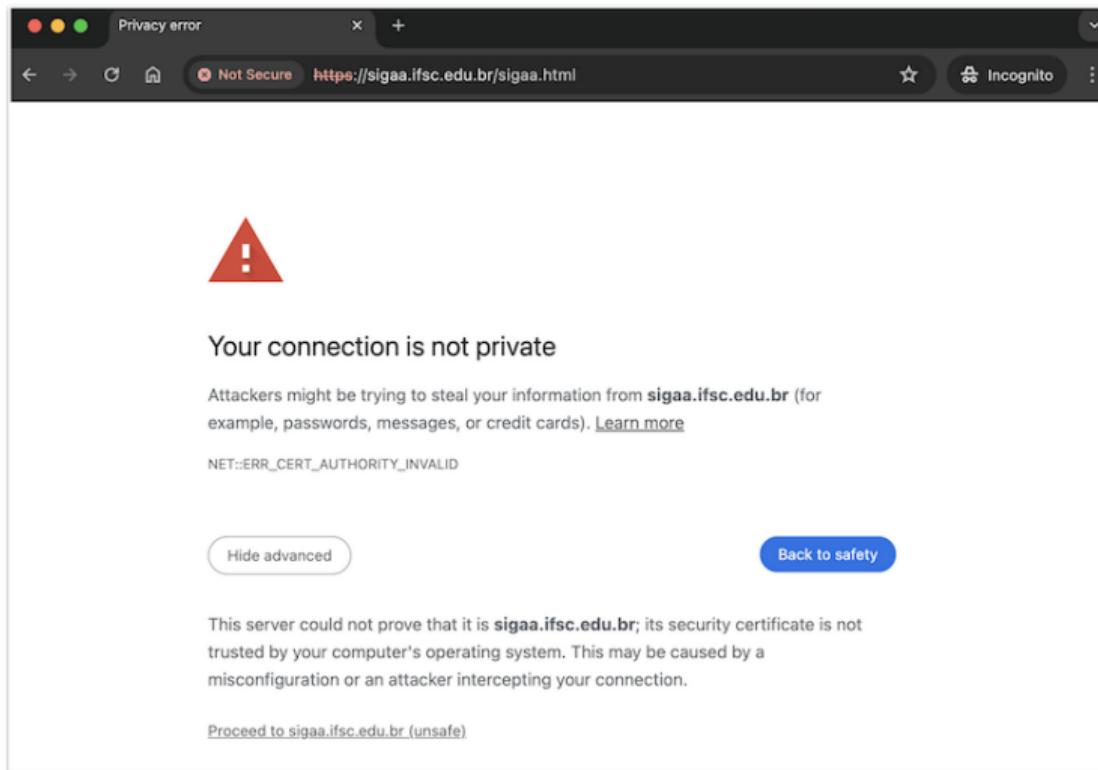
- Não garante a autenticidade do servidor para o cliente
- Suscetível a ataque do homem no meio e de personificação

Certificados autoassinados II



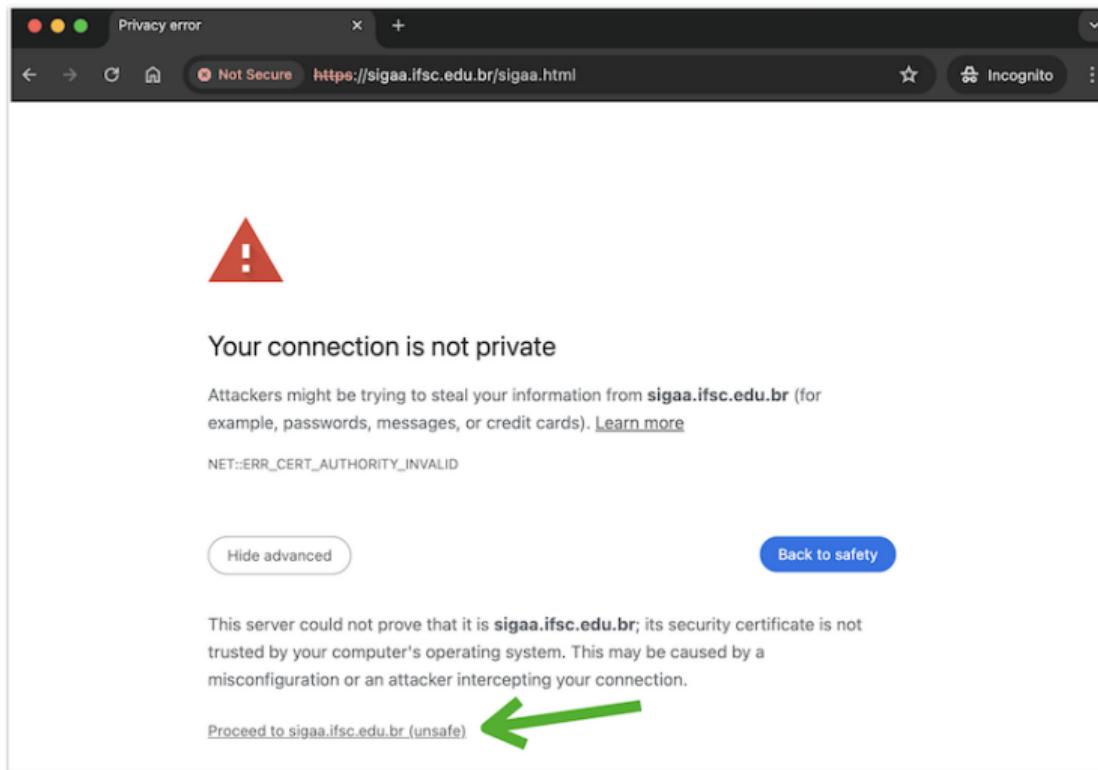
Site falso com certificado autoassinado

Exemplo: Acessando o SIGAA <https://sigaa.ifsc.edu.br>



Site falso com certificado autoassinado

Exemplo: Acessando o SIGAA <https://sigaa.ifsc.edu.br>



Site falso com certificado autoassinado

Exemplo: Acessando o SIGAA <https://sigaa.ifsc.edu.br>

The screenshot shows a web browser window with the title "SIGAA - Sistema Integrado de Gestão de Atividades Acadêmicas". The address bar indicates the URL is <https://sigaa.ifsc.edu.br/sigaa.html>, which is marked as "Not Secure". The page content is as follows:

ATENÇÃO!
O sistema diferencia letras maiúsculas de minúsculas APENAS na senha, portanto ela deve ser digitada da mesma maneira que no cadastro.

Navigation menu:

- SIGAA (Acadêmico) [highlighted]
- SIPAC (Administrativo)
- SIGRH (Recursos Humanos)
- SIGAdmin (Administração e Comunicação)

Forgot login? [Clique aqui para recuperá-lo.](#)
Forgot password? [Clique aqui para recuperá-la.](#)

ENTRAR NO SISTEMA

Usuário:
Senha:

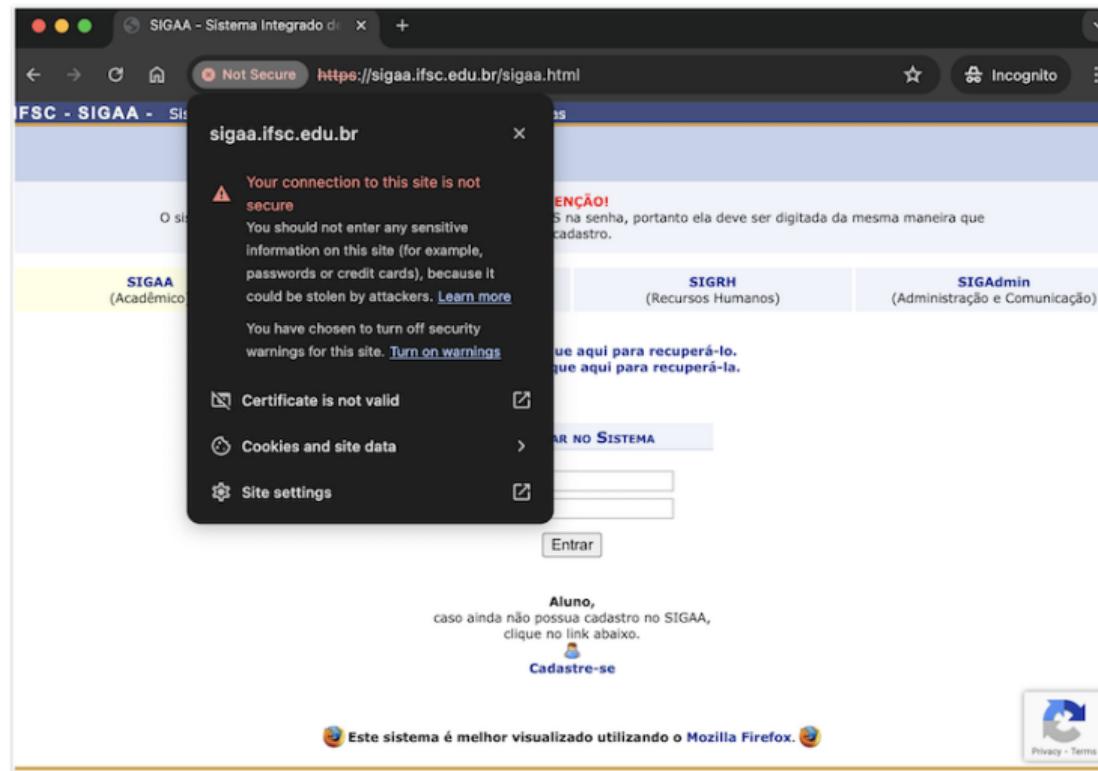
Aluno,
caso ainda não possua cadastro no SIGAA,
clique no link abaixo.
 [Cadastre-se](#)

Este sistema é melhor visualizado utilizando o Mozilla Firefox.

Privacy - Terms

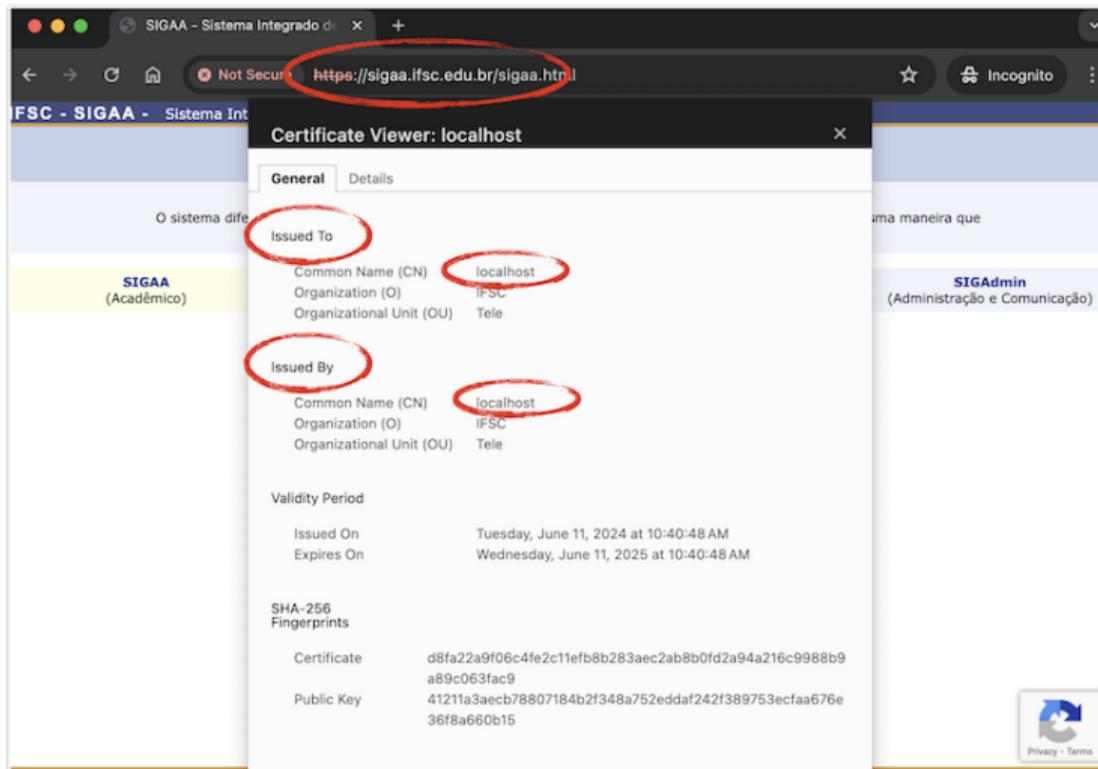
Site falso com certificado autoassinado

Exemplo: Acessando o SIGAA <https://sigaa.ifsc.edu.br>



Site falso com certificado autoassinado

Exemplo: Acessando o SIGAA <https://sigaa.ifsc.edu.br>



Site falso com certificado autoassinado

Exemplo: Acessando o SIGAA <https://sigaa.ifsc.edu.br>

The screenshot shows a web browser window with the title "SIGAA - Sistema Integrado de Gestão de Atividades Acadêmicas" and the URL "sigaa.ifsc.edu.br/sigaa/verTelaLogin.do". The page content is identical to the official SIGAA login page, featuring a warning about case sensitivity, navigation links for SIGAA, SIPAC, SIGRH, and SIGAdmin, and a login form with fields for "Usuário" and "Senha". Below the form, there is a link for new users to "Cadastrar-se". The bottom of the page includes a note about Mozilla Firefox and links for "Privacy - Terms".

ATENÇÃO!

O sistema diferencia letras maiúsculas de minúsculas APENAS na senha, portanto ela deve ser digitada da mesma maneira que no cadastro.

SIGAA
(Acadêmico)

SIPAC
(Administrativo)

SIGRH
(Recursos Humanos)

SIGadmin
(Administração e Comunicação)

Esqueceu o login? [Clique aqui para recuperá-lo.](#)
Esqueceu a senha? [Clique aqui para recuperá-la.](#)

ENTRAR NO SISTEMA

Usuário:
Senha:

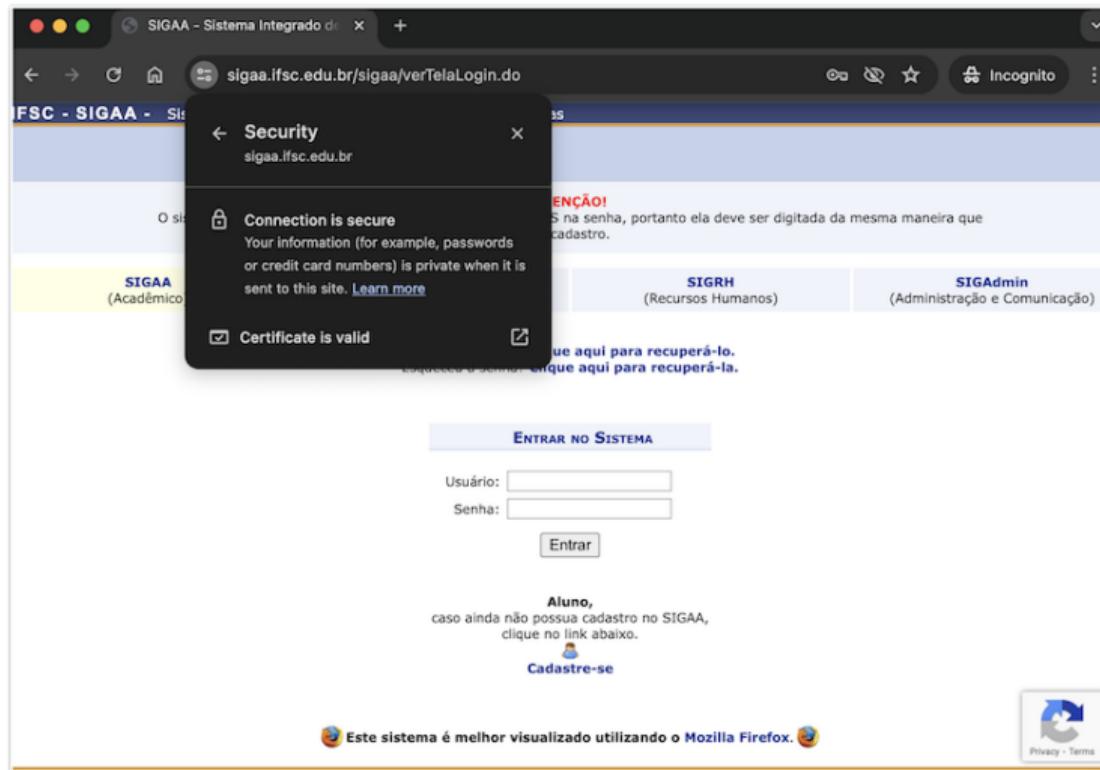
Aluno,
caso ainda não possua cadastro no SIGAA,
clique no link abaixo.
 [Cadastrar-se](#)

Este sistema é melhor visualizado utilizando o Mozilla Firefox.

Privacy - Terms

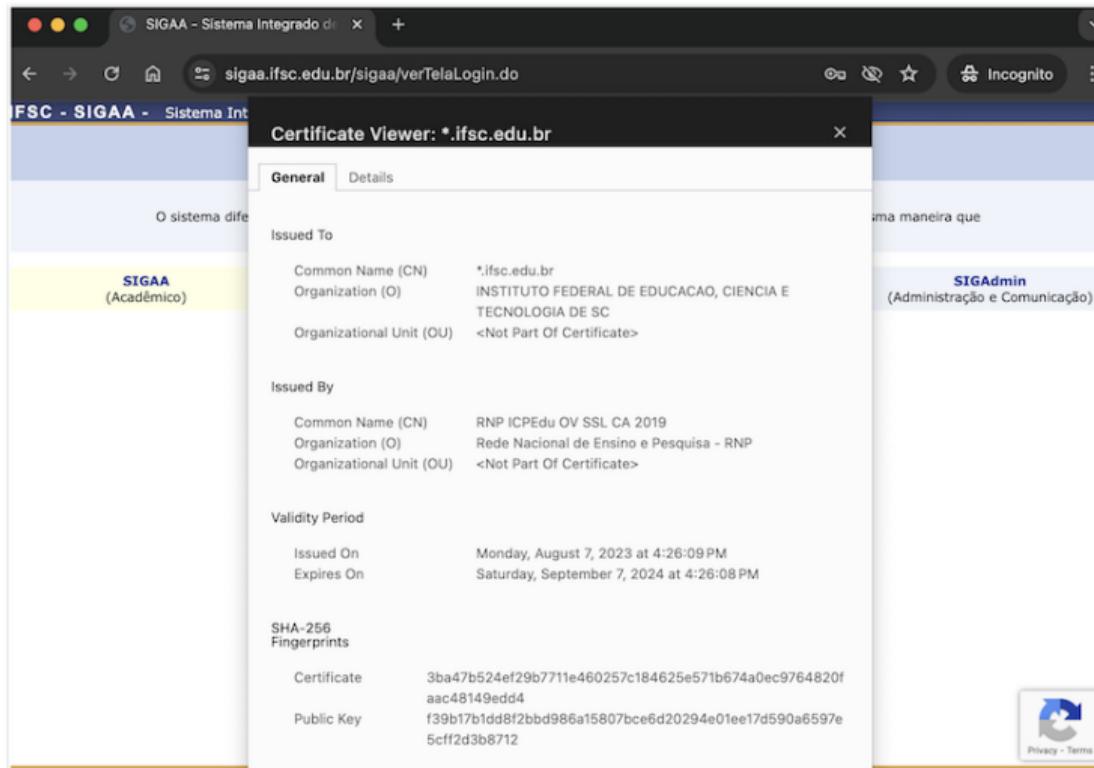
Site falso com certificado autoassinado

Exemplo: Acessando o SIGAA <https://sigaa.ifsc.edu.br>



Site falso com certificado autoassinado

Exemplo: Acessando o SIGAA <https://sigaa.ifsc.edu.br>



Infraestrutura de Chaves Públicas (ICP) I

Hierarquia de confiança para emissão de certificados digitais

Definição

Conjunto de entidades, políticas, procedimentos e tecnologias que viabilizam a emissão e o gerenciamento de certificados digitais

Infraestrutura de Chaves Públicas (ICP) II

Hierarquia de confiança para emissão de certificados digitais

- **Autoridades Certificadoras (AC)**

- Responsável por emitir certificados digitais para entidades

- **Autoridades de Registro (AR)**

- Responsável por verificar a identidade do solicitante do certificado digital

- **Autoridades de Carimbo do Tempo (ACT)**

- Responsável por atestar a data e a hora em que uma mensagem foi assinada

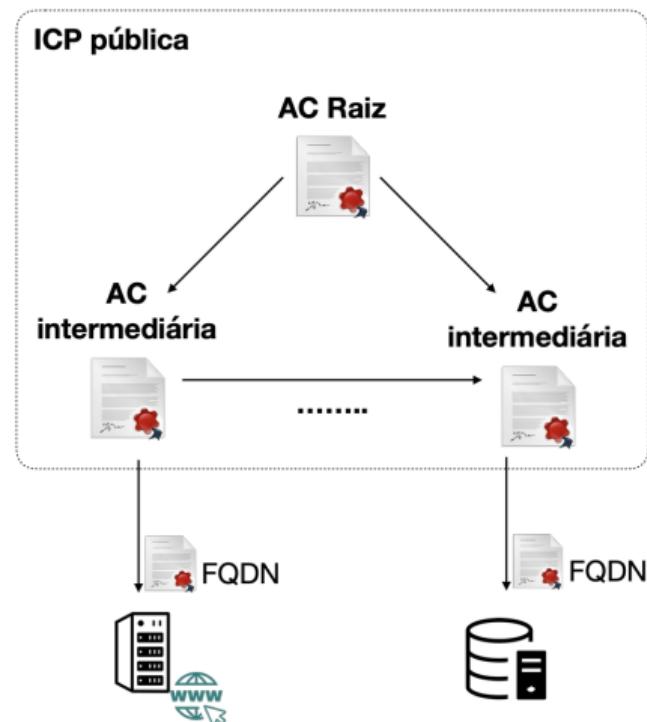
- **Lista de certificados revogados (CRL)**

- Para verificar se um certificado foi revogado

Infraestrutura de Chaves Públicas (ICP) III

Hierarquia de confiança para emissão de certificados digitais

- AC Raiz emite certificados para as ACs intermediárias
- ACs intermediárias emitem certificados para as entidades
- O cliente (navegador, S.O., etc) confia na AC Raiz e nas ACs intermediárias

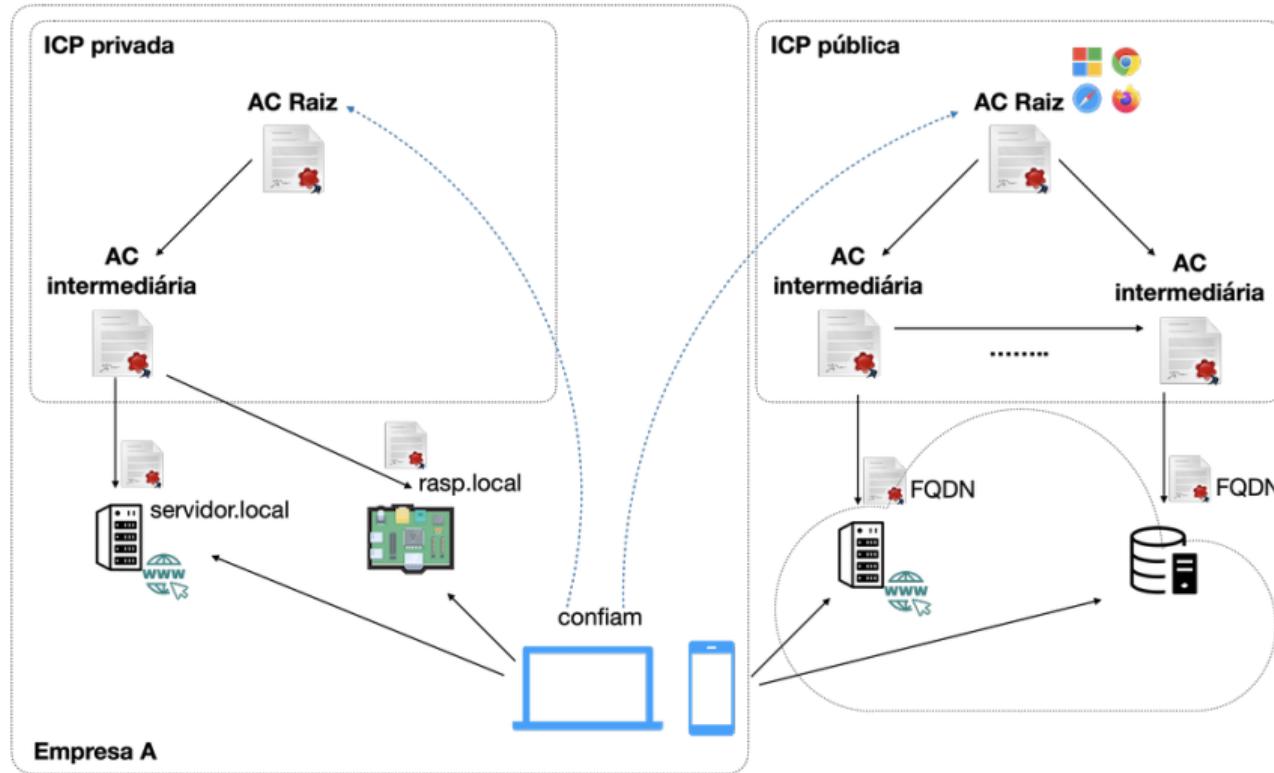


ICP pública e privada

- ICP pública é controlada por uma entidade pública ou privada
 - Exemplos: Let's Encrypt, DigiCert, GoDaddy, ICP-Brasil
- ICP privada é controlada pela própria organização
 - Controle total sobre identidade e verificação de credenciais
- Para cenários específicos, uma ICP privada pode ser mais adequada do que uma ICP pública ou certificados autoassinados
 - Dispositivos IoT
 - Servidores em uma rede corporativa e com nome de domínio interno (e.g. servidor.local)

ICP pública e privada

ICP privada da controle total sobre identidade e verificação de credenciais



Autoridade Certificadora (AC) de uma ICP

Discussão

■ Quando e como a confiança em um AC pública é estabelecida?

- Chaves das ACs são distribuídas com o sistema operacional e navegador
- Se você confia nesses softwares, então você confia nas ACs que eles confiam
- Você pode adicionar manualmente ACs confiáveis no S.O. ou navegador

■ Como a confiança em uma AC privada é estabelecida?

- A AC privada emite um certificado autoassinado para si mesma
- Adicionar manualmente o certificado da AC no S.O. ou navegador

Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)

Regulamentada pela Medida Provisória nº 2.200-2/2001¹

- Cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão ou empresa
- e-CPF e e-CNPJ são certificados digitais emitidos pela ICP-Brasil
- Tipos de certificados
 - A1 – arquivo armazenado no computador e tem validade de 1 ano
 - A3 – armazenado em cartão, token criptográfico ou diretamente na nuvem (HSM remoto) e tem validade de 3 anos

¹https://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm

Infraestrutura de Chaves Públicas

Centralização de confiança e os riscos associados

■ Riscos associados se uma AC for comprometida

- Todos os certificados emitidos por ela são comprometidos
- Em 2011 DigitNotar² foi comprometida e certificados falsos foram usados contra usuários iranianos para permitir MITM nos domínios da Google

■ Confiança nos fabricantes de sistemas operacionais e navegadores

- Microsoft, Apple, Google, Mozilla, etc.
- Em 2019 Mozilla e Google baniram a AC DarkMatter de seus navegadores por violações de confiança
- Em 2024 Google³ remove a Entrust da lista de ACs confiáveis

²<https://blog.mozilla.org/security/2011/08/29/fraudulent-google-com-certificate>

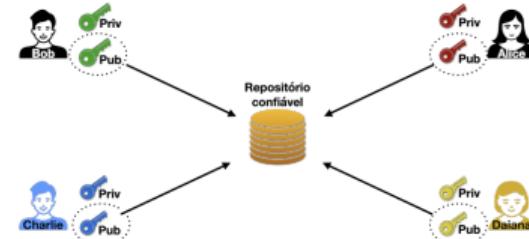
³<https://security.googleblog.com/2024/06/sustaining-digital-certificate-security.html>

Redes de confiança (*Web of Trust*)

- Proposto 1992 por Phil Zimmermann para o PGP (*Pretty Good Privacy*)
 - Inicialmente para assinatura e criptografia de e-mails
 - Atualmente é usado para verificar a autenticidade de softwares
- Usuários confiam em chaves públicas sem depender de uma AC
 - Cada usuário pode assinar a chave pública de outro usuário e publicar a assinatura
 - Confiança é baseada na rede de assinaturas (direta e indireta)
- Implementações: PGP, GnuPG e OpenPGP

- Repositórios de chaves públicas e assinaturas

- <https://keys.openpgp.org>
 - <https://keyserver.ubuntu.com>



Assinatura eletrônica

Assinatura digital

Criptografia assimétrica

- Permite verificar a autoria e a integridade do documento

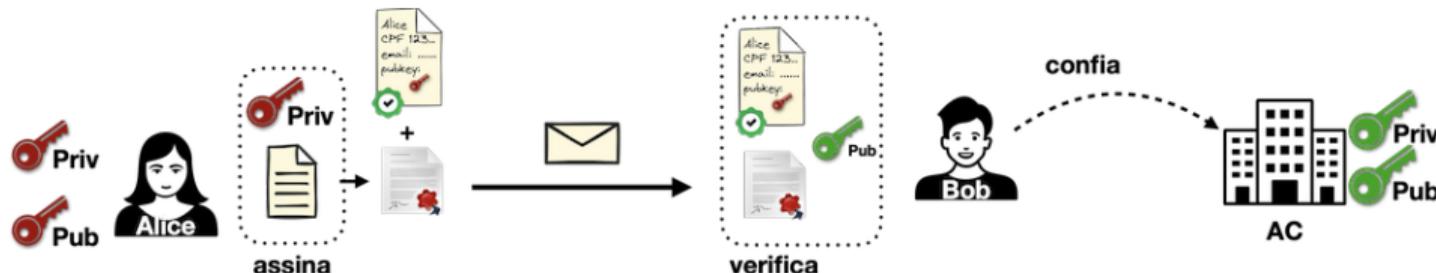
- Sobre o documento é aplicada uma função de resumo criptográfico e o resultado é assinado com a chave privada do signatário

- A assinatura digital fornece o não-repúdio

- O signatário não pode negar que assinou a mensagem, uma vez que garante que sua chave privada permanece em segredo

- Vincula o certificado digital ao documento que está sendo assinado

- A confiança na assinatura digital depende da confiança no certificado digital



Assinatura eletrônica

Legislação brasileira

- **Lei nº 14.063, de 23 de Setembro de 2020⁴,**
 - *"dispõe sobre as regras para uso das assinaturas eletrônicas nas interações entre pessoas e instituições privadas com os entes públicos e entre os próprios órgãos e entidades públicas"*
 - *"Para os demais casos de uso de assinaturas eletrônicas deve-se observar a Medida Provisória nº 2.200-2/2001⁵"*

Assinatura eletrônica

- Termo mais amplo, pois deixa em aberto as tecnologias que podem ser utilizadas para assinar documentos eletrônicos
- **Assinatura digital** é um tipo de assinatura eletrônica que utiliza criptografia assimétrica

⁴http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14063.htm

⁵https://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm

Assinatura eletrônica no Brasil

Classificação

■ Assinatura eletrônica simples

- Permite identificar seu signatário e associa dados a outros dados em formato eletrônico do signatário

■ Assinatura eletrônica avançada

- Faz uso de certificados digitais não emitidos pela ICP-Brasil ou outro meio de comprovação de autoria e integridade de documentos em forma eletrônica, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento
- Assinatura GOV.BR⁶ é um exemplo de assinatura eletrônica avançada

■ Assinatura eletrônica qualificada

- Faz uso de certificado digital emitido no âmbito da ICP-Brasil, nos termos do § 1º do art. 10 da Medida Provisória nº 2.200-2, de 24 de agosto de 2001

⁶<https://www.gov.br/iti/pt-br/assuntos/assinatura-eletronica-avancada>

Assinatura eletrônica no Brasil

Lei nº 14.063, de 23 de Setembro de 2020

- Os três tipos de assinatura eletrônica caracterizam o nível de confiança sobre a identidade e a manifestação de vontade de seu titular
- A **assinatura eletrônica qualificada** é a que possui nível mais elevado de confiabilidade a partir de suas normas, de seus padrões e de seus procedimentos específicos
- O documento com a assinatura digital tem a mesma validade de um documento com assinatura física⁷

⁷<https://www.gov.br/governodigital/pt-br/identidade/assinatura-eletronica>

Assinatura de próprio punho em documento físico I

Documento original em papel

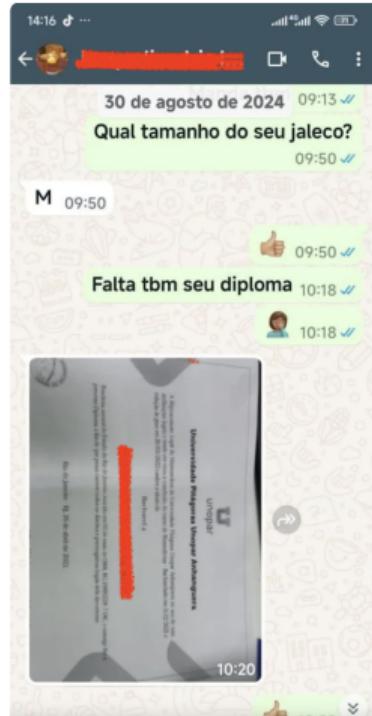


Fonte: Acervo pessoal. Documento físico digitalizado

- Como garantir que a assinatura é autêntica?
- Seria fácil falsificar a assinatura?
- Qual a garantia de que o documento não foi alterado depois de assinado?
- Como garantir que o documento é autêntico?

Assinatura de próprio punho em documento físico II

Documento original em papel



- Formação de funcionária que assinou exames errados de HIV é incerta (15/10/2024)
- <https://www.cnnbrasil.com.br/nacional/formacao-de-funcionaria-que-assinou-exames-errados-de-hiv-e-incerta-entenda/>

Assinatura de próprio punho em documento nato digital I

Assinatura de próprio punho é digitalizada e anexada a um documento digital



Fonte: Acervo pessoal. Documento digital com assinatura de próprio punho digitalizada

- Como impedir que a imagem da assinatura seja copiada para outro documento?
- Qual a garantia de que o documento não foi alterado depois de assinado?
- Como garantir que o documento é autêntico?

Assinatura de próprio punho em documento nato digital II

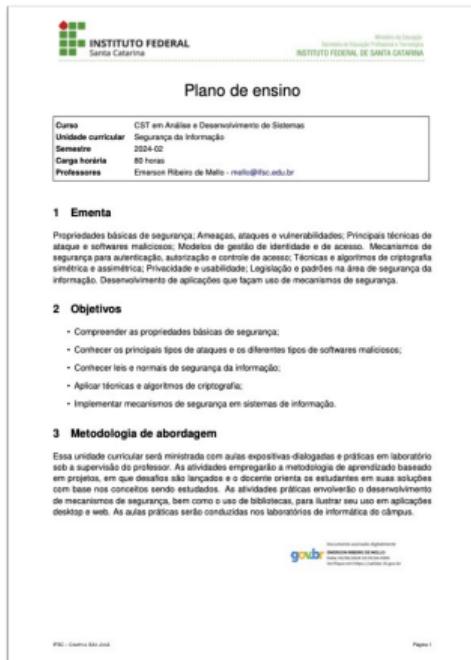
Assinatura de próprio punho é digitalizada e anexada a um documento digital

Embora reconheça que as rubricas nos documentos seja sua, [REDACTED] destaca que as assinaturas eletrônicas foram coletadas pela empresa assim que foi contratada e que este era um procedimento padrão para todos os funcionários

15/10/2024.⁸

⁸<https://oglobo.globo.com/rio/noticia/2024/10/15/orgaos-infectados-faculdade-nao-reconhece-diploma-de-tecnica-e-laboratorio-diz-que-ela-apresentou-o-documento-falso.ghtml>

Assinatura eletrônica em documento nativo digital



Fonte: Acervo pessoal. Documento digital assinado digitalmente com <https://assinador.iti.gov.br>

- Garante a integridade do documento
- Como saber que o documento foi assinado digitalmente?
- Como garantir que a assinatura é autêntica?
 - <https://validar.iti.gov.br>
- Como garantir a identidade do signatário?
 - Certificado digital emitido por uma Autoridade Certificadora (AC) confiável
- Como garantir o horário da assinatura?
 - Carimbo do tempo de uma Autoridade de Carimbo do Tempo (ACT)

Assinatura eletrônica em documento nativo digital

The image contains two screenshots of Adobe Acrobat Reader. The top screenshot shows the 'Visualizador de certificados' (Certificate Viewer) dialog box. It displays a list of actions that can be performed with a certificate, including 'Assinar documentos ou dados', 'Certificar documentos', 'Executar conteúdo dinâmico que esteja incorporado em um documento certificado', 'Executar JavaScripts de alto privilégio que estejam incorporados em um documento certificado', and 'Operações privilegiadas do sistema (conexão em rede, impressão, etc.)'. The bottom screenshot shows the 'Assinaturas' (Signatures) panel, which lists a single certificate for 'EMERSON RIBEIRO DE MELLO'. It includes information about the signature's validity and details about the signer.

Fonte: Acervo pessoal. Capturas de tela do Adobe Acrobat Reader

- PDF assinado digitalmente com <https://assinador.iti.br>
 - Pessoa que assinou com conta no nível ouro^a
- Adobe Acrobat indica que
 - o documento não foi alterado
 - não reconhece a identidade do signatário
- **Certificado digital** não foi emitido por uma AC confiável pelo Adobe Acrobat

^a<https://www.gov.br/governodigital/pt-br/identidade/conta-gov-br/niveis-da-conta-govbr>

Curiosidade

Diploma Digital – Ministério da Educação (MEC)⁹

- Documento nato-digital, ou seja, aquele que adota o formato digital desde a sua origem, tendo a mesma validade jurídica do documento físico, em papel
 - Para diplomas de graduação
- Emitido no formato *Extensible Markup Language* (XML), valendo-se da assinatura eletrônica avançada no padrão *XML Advanced Electronic Signature* (XadES)
 - Versão em PDF é gerada para fins de visualização (pode conter QR Code para facilitar a verificação)
- A assinatura digital é feita por um certificado digital ICP-Brasil emitido para a instituição de ensino

⁹<http://portal.mec.gov.br/diplomadigital/>

Referências

- Alguns ícones presentes nas imagens foram obtidos de <https://uxwing.com> ou de <https://flaticon.com>