UM ESTUDO SOBRE CERTIFICADOS DIGITAIS COMO SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO

Emerson Henrique Soares Silva

Orientação:
Prof. Ms. Rodrigo Almeida dos Santos

Agenda

- Introdução
- Certificados Digitais
  - O que são Certificados Digitais
  - Critérios de Segurança Garantidos
  - Tipos de Certificados Digitais
- ICP ou PKI
  - ICP-Brasil
  - Estrutura da ICP-Brasil
  - Teia de Confiança
  - Obtendo um Certificado Digital
  - Cuidados com o certificado
- Exemplos de uso dos Certificados Digiais
- Conclusão
- Dúvidas
- Referências
- Links

Introdução

- Internet + Informação = Agilidade dos processos e Velocidade de Circulação da informação
- Antes da Internet = Qualquer movimentação financeira e de documentos eram feitas mão a mão, de forma pessoal e de corpo presente
- Com a Internet = Os documentos e diversas informações circulam por redes de computadores e são compostos por *bits*
- Com a Internet += riscos de interceptação e roubo de informações, fabricação de informações falsas, interrupções de serviços, modificação de informações, etc.

Introdução

- Meu objetivo
  - Apresentar, baseado em levantamento bibliográfico, os Certificados Digitais como solução de segurança da informação.

- Os certificados podem ser e são usados no controle de acesso de usuários de site, como e-CAC (Centro Virtual de Atendimento ao Contribuinte), que é um serviço oferecido pela Redeita Federal do Brasil, onde os acessos só são possíveis para usuários que possuem certificados e-CPF ou e-CNPJ

- Uma aplicação bastante conhecida são os certificados digitais, que, de acordo com a analogia de RIBEIRO [3], são equivalentes aos carimbos e selos emitidos por cartórios para registro de firma de documentos, já que ambos possuem o objetivo de validar documentos

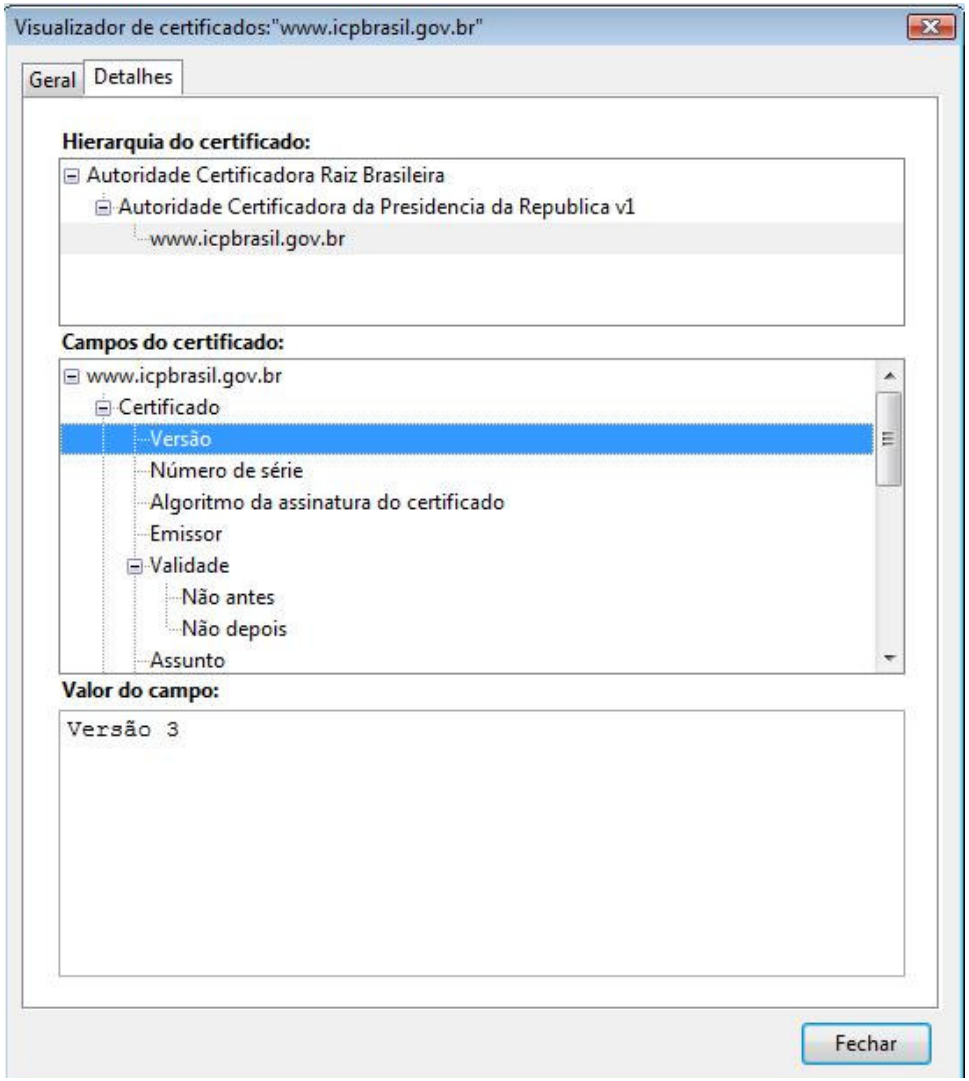
Certificados Digitais

- A proposta dos certificados digitais é promover alguns serviços de segurança como:
  - Confidencialidade
    - Garantia de que a informação só será acessada por quem possui autorização.
  - Integridade
    - Garantia de que a informação não foi modificada de alguma forma por quem não tinha autorização.
  - Autenticidade
    - Garantia de que a informação permanece como original e integra.
  - e Não-Repudiação de informações
    - Garantia de que, se a informação for passada é possível saber quem o fez, e este não pode negar que fez.
- Implementam o conceito de Criptografia Assimétrica

O que são Certificados Digitais?

- Documentos eletrônicos que identificam uma pessoa, uma instituição, uma máquina ou uma aplicação na internet. (RIBEIRO, 2007)[3]
- Possuem um padrão, o X.509 – Versão 3, padrão criado pelo ITU (International Telecommunication Union) e adaptado para internet pelo grupo PKIX da *Internet Engineering Task Force* (IETF)
- Possuem um par de chaves criptográficas (pública e privada) relacionadas a cada certificado
- São emitidos por organizações chamadas Autoridades Certificadoras (ACs)

Exemplo de Certificado Digital padrão X.509



Criptografia Assimétrica

- A criptografia é a codificação de textos de forma que ele fique incompreensível.
- Seja:
  - T = Texto puro
  - K = chave de criptografia
  - C = Texto cifrado
  - E(x,y) = função de encriptação
  - D(x,y) = função de decriptação
- Temos:
  - E(K,T) = C "A encriptação do texto T utilizando a chave K resulta em um texto cifrado C"
  - D(K,C) = T "A decriptação do texto cifrado C utilizado uma chave K resulta no texto puro T"
- Na Criptografia Assimétrica as chaves para encriptar (K_e) e decriptar (K_p) um texto são diferentes ou seja, $K_e \neq K_p$
- Então temos:
  - E(K_e,T) = C "A encriptação do texto T utilizando a chave K resulta em um texto cifrado C"
  - D(K_p,C) = T "A decriptação do texto cifrado C utilizado uma chave K resulta no texto puro T"
- Ou
  - E(K_p,T) = C "A encriptação do texto T utilizando a chave K resulta em um texto cifrado C"
  - D(K_e,C) = T "A decriptação do texto cifrado C utilizado uma chave K resulta no texto puro T"

Exemplo de Criptografia Assimétrica

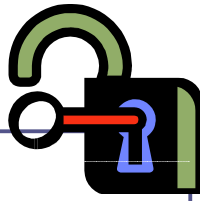
- ANDRÉ
- $E(k_{eA},T) = C$

C

C

- YdjfneBuyd
- ∑ └∞∫ΦβNηЩ
- ŶţŽ¥¼¿±Ядй

- PAULO
- $E(k_{pA},C) = T$



Texto

Critétios de Segurança Garantidos

- Os algoritmos criptográficos assimétricos garatem integridade, confidencialidade, podem garantir a autenticidade e a não-repudiação

- Quando um emissor criptografa um documento com sua chave privada, apenas quem tiver a sua chave pública poderá decriptar o documento, e dessa forma quem possui a chave pública tem a certeza de quem enviou o documento e de que este está autêntico.

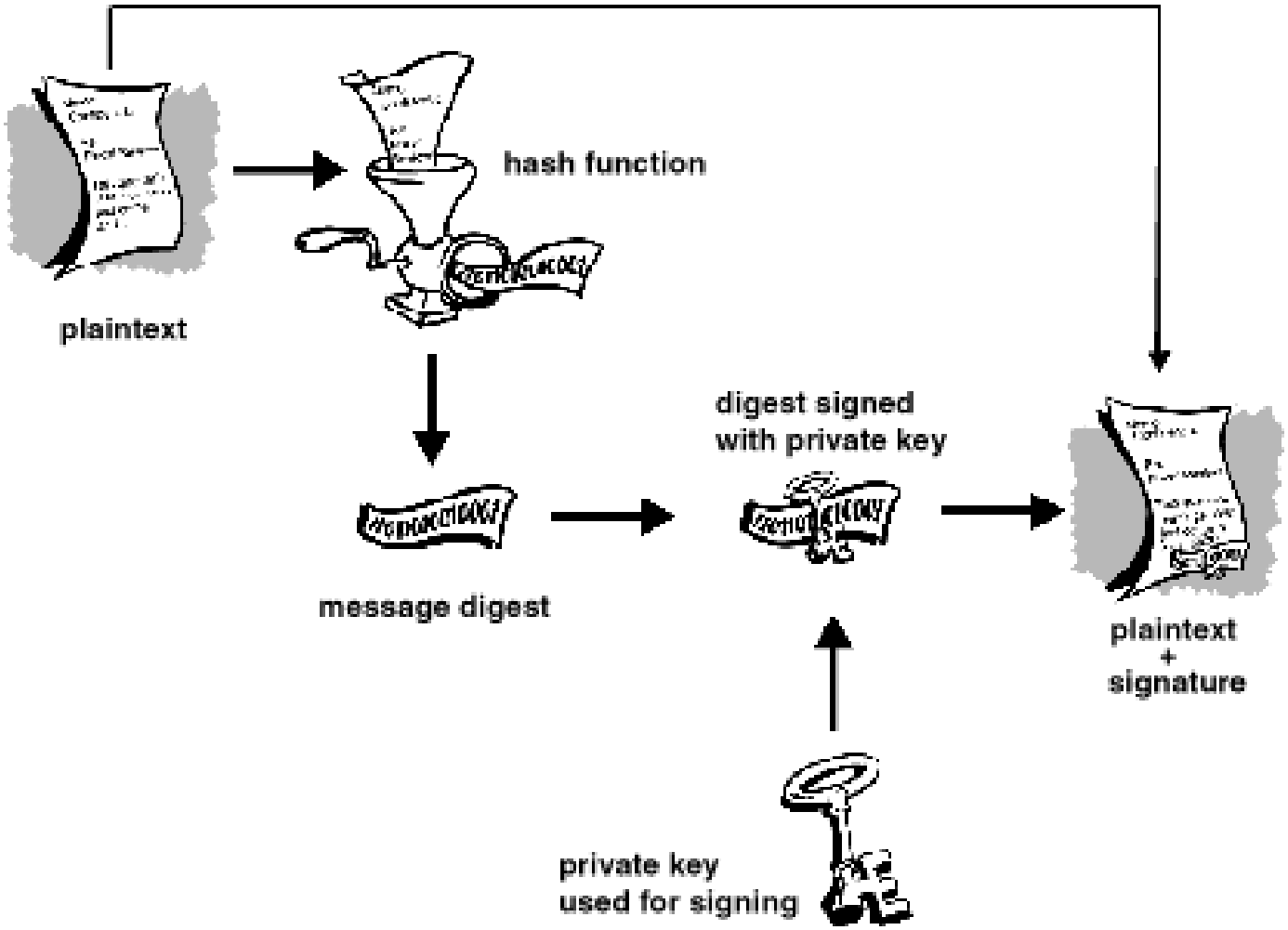
Assinatura Digital

- É uma das aplicações mais conhecidas do certificado digital
- Une os conceitos de criptografia assimétrica aos de funções *hash*
- Função Hash é uma técnica de criptografia de via única, que utiliza de algoritmos matemáticos bastante complexos em cima dos caracteres de um texto ou bits de um documento para gerar um valor de tamanho fixo chamado valor hash.

Assinatura Digital

- Funciona assim:
  - *Seja Hs a função Hash. Seja C(K, T) a função responsável por criptografar o texto T utilizando a chave K. Seja D(K,T) a função responsável por decriptografar o texto T utilizando a chave K.*
- *Cenário:*
  - *O usuário A deseja enviar o texto T assinado digitalmente para o usuário B. O usuário B possui K_pA, que é a chave pública do usuário A. A chave privada do usuário A é K_eA – e somente quem possui essa chave é o próprio usuário A. O usuário A envia ao usuário B o texto T, e em anexo o código resultante da seguinte função: $C(K_eA, Hs(T)) = X$. O usuário B, ao receber a mensagem, deverá primeiro aplicar a função de decriptografia sobre X: $D(K_pA, X) = Hs(T)$. Em seguida o usuário B deverá aplicar a função Hash sobre o texto T, e verificar se o resultado que ele obteve é igual ao resultado passado pelo usuário A*

Assinatura Digital



Tipo de Certificados Digitias

- Podem ser armazenados em Tokens, SmartCards ou arquivos eletrônicos.

- São classificadas em dias séries, quanto ao uso e nível de segurança implantadas:
  - Série A
    - Certificados utilizados como assinatura digital para identificação na web.
  - Série S
    - Utilizados na codificação de documentos, base de dados, mensagens sigilosas.

Tipo de Certificados Digitias

Tipo de Certificado	Chave Criptográfica			Validade Máxima (anos)
	Tamanho de bits	Processo de Geração	Mídia Armazenadora	
A1 e S1	1024	Software	Arquivo	1
A2 e S2	1024	Software	Smartcard ou token, sem capacidade de geração de chave	2
A3 e S3	1024	Hardware	Smartcard ou token, com capacidade de geração de chave	3
A4 e S4	2048	Hardware	Smartcard ou token, com capacidade de geração de chave	3

Os mais comuns são os A1 e A3.

ICP ou PKI

- Uma Infra-estrutura de Chaves Públicas (ICP) ou PKI (Public Key Infrastructure) é um conjunto de entidades, padrões técnicos e regulamentos, elaborados para suportar um sistema criptográfico com base em certificados digitais. [1]

- No Brasil temos a ICP-Brasil

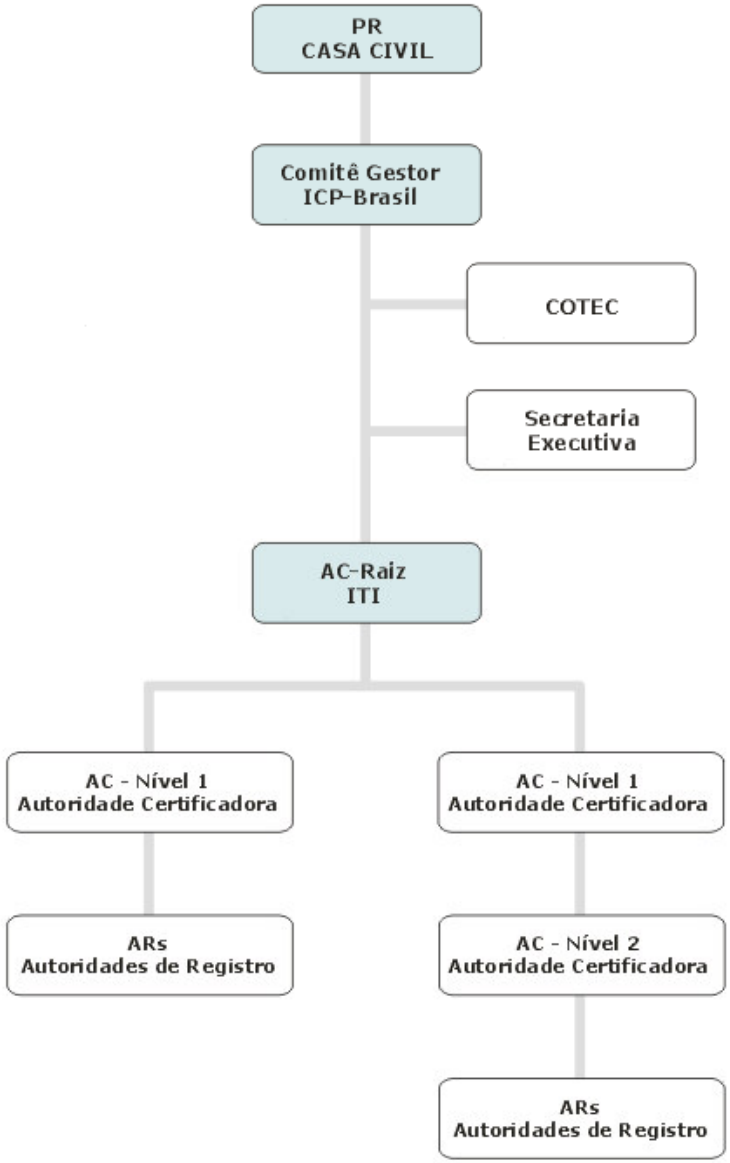
ICP-Brasil

- Foi criada após a percepção da Presidência da República de que deveria regulamentar as atividades de certificação digital no país.

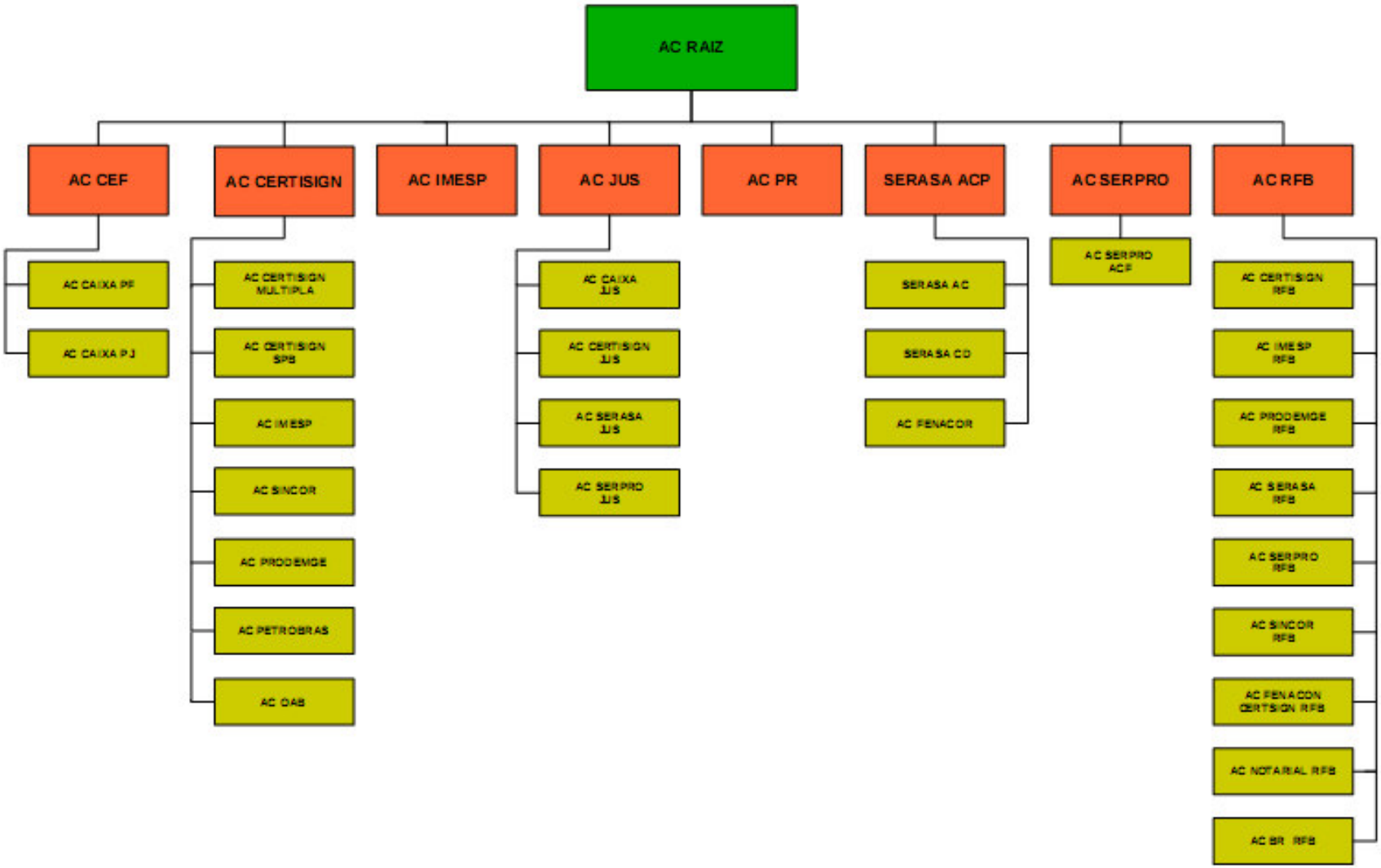
- Foi instituída pela Medida Provisória 2.200-2, de 24 de Agosto de 2001, que criou o Comitê Gestor da ICP-Brasil, a Autoridade Certificadora Raiz, que é o Instituto Nacional de Tecnologia da Informação (ITI), e as demais entidades que compõem a estrutura da ICP-Brasil.

- A partir dessa medida, também foram regulamentadas as atividades das entidades integrantes dessa ICP [1]

Estrutura da ICP-Brasil



Estrutura da ICP-Brasil



Teia de Confiança

- Essa teia é a relação de confiança que há entre a AC-Raiz, as demais ACs e os portadores de certificados.

- Os certificados emitidos por ACs garantem a que a pessoa que te envia o certificado é quem diz ser, por tanto é uma pessoa confiável.

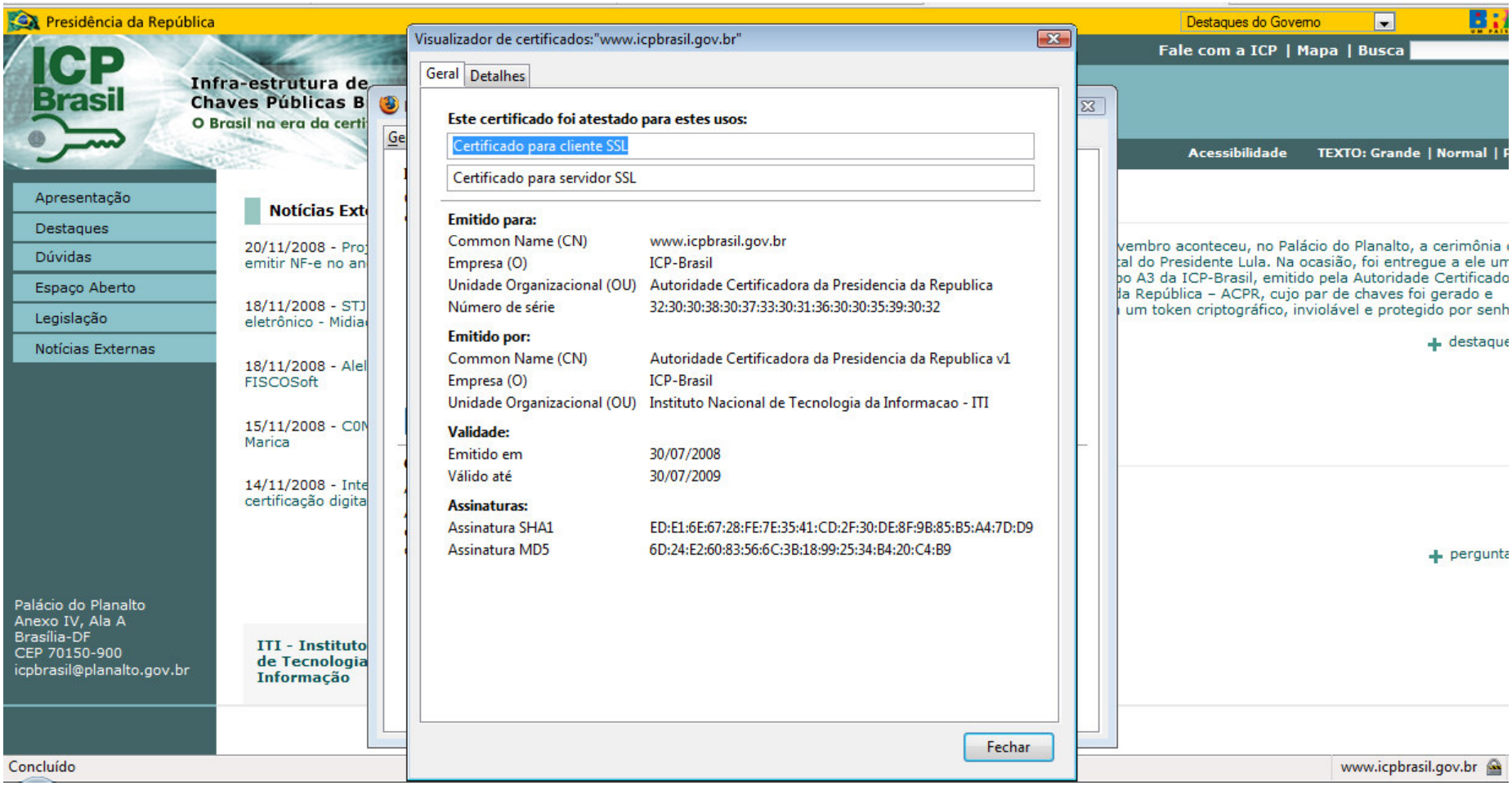
Obtendo um Certificado Digital

Cuidados com o Certificado

- Proteja a senha do seu certificado, ela é única e não pode ser recuperada ;
- Em caso de perda, peça revogação do seu certificado;
- Solicite novo certificado, arcando com todos os custos e passando pelo mesmo processo de solicitação do certificado anterior;
- Atualize a sua chave pública onde ela estiver distribuída, passando a nova adquirida;

Alguns exemplos de uso

Certificados para Servidores WEB



Alguns exemplos de uso

Certificados para WEB Mail

- Certificados para aplicações cliente de correio eletrônico.
- A aplicação tem que suportar os certificados.
- A maioria dos clientes de E-mail em interface web ainda não suportam os certificados digitais.

Alguns exemplos de uso

Certificados Controle de Acesso

- O e-CAC é um exemplo de uso dos certificados digitais para controle de acesso

- Para accessar é necessário possuir um –CPF ou e-CNPJ

- Essa aplicação da receita Federal do Brasil dá acesso ao contribuite a documentos sigilosos, e é um espaço para que ele envie a RFB documentos relativos as suas contribuições e seus tributos.

Conclusão

- Atingido os objetivos de apresentar os certificados digitais como uma solução de segurança da informação.
- Solução que garante serviços de segurança básicos, como confidencialidade, integridade, autenticidade e não-repudiação, e permitem que a internet seja usada de forma mais segura, eliminando a timidez no seu uso para transações confidenciais e sigilosas, como no e-CAC da RFB.
- Foi apresentada a ICP-Brasil e como essa infra-estrutura envolve em uma teia de confiança os portadores de certificados digitais

Dúvidas

Referências

- [1] Infra-estrutura de Chave Pública Brasileira - ICP-Brasil. Disponível em: <https://www.icpbrasil.gov.br> Acesso em: 11 nov. 2008.
- [2] Instituto Nacional de Tecnologia da Informação - ITI. Disponível em: <http://www.iti.gov.br/twiki/bin/view/Certificacao/CertificadoConceitos> Acesso em: 11 nov. 2008.
- [3] RIBEIRO, Gisele. **Como funciona o certificado digital.** HowStuffWorks (ComoTudoFunciona). Disponível em: <http://informatica.hsw.uol.com.br/certificado-digital.htm> Acesso em: 09 nov. 2008.
- [4] Certisign. Disponível em: <https://www.certisign.com.br/> Acesso em: 12 nov. 2008.
- [5] Movimento Internet Segura. Portal INTERNET SEGURA. Disponível em: <http://www.internetsegura.org > Acesso em: 15 nov. 2008.
- [6] MATOS, Manoel. **Ser quem diz ser. Esta é a questão.** Moviento Internet Segura. Portal INTERNET SEGURA. Disponível em: <http://www.internetsegura.org/noticias/22112006.asp> Acesso em: 15 nov. 2008.
- [7] ALECRIM, Emerson. **Assinatura Digital e Certificação Digital.** Info Wester. 2005. Disponível em: <http://www.infowester.com/assincertdigital.php> Acesso em: 09 nov. 2008.
- [8] JANUÁRIO, Larissa. **Tutorial: Saiba tudo sobre certificação digital.** W News. 2007. Disponível em: <http://wnews.uol.com.br/site/noticias/materia_especial.php?id_secao=17&id_conteudo=264> Acesso em: 09 nov. 2008.
- [9] BRASIL, Presidência da República, Casa Civil, Subchefia para Assuntos Jutídicos. **MEDIDA PROVISÓRIA Nº2.200-2, DE 24 DE AGOSTO DE 2001**. Disponível em: <https://www.planalto.gov.br/ccivil_03/MPV/Antigas_2001/2200-2.htm> Acesso em: 16 nov. 2008.

Links

- https://www.icpbrasil.gov.br
- http://www.iti.gov.br/
- Para baixar esse material:
  - http://emersonhss.eti.br

Obrigado!

UM ESTUDO SOBRE CERTIFICADOS DIGITAIS COMO SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO

Emerson Henrique Soares Silva

Orientação:
Prof. Ms. Rodrigo Almeida dos Santos