Gestão de documentos nas organizações: fundamentos, sistemas e tecnologias

Submódulo 4

Novas perspectivas tecnológicas na gestão de documentos e arquivos

Assinatura, Certificação e Tempestividade digital

prof. Maurício B. Almeida
mba@eci.ufmg.br
http://mba.eci.ufmg.br

1

Roteiro da apresentação:

Introdução

Fundamentos básicos

- Aspectos tecnológicos, jurídicos e culturais da certificação digital
- Requisitos da assinatura em documentos eletrônicos
- Conceitos de assinatura: eletrônica, digitalizada, biométrica e digital

ICP-Infraestrurura de chaves públicas

Tempestividade digital

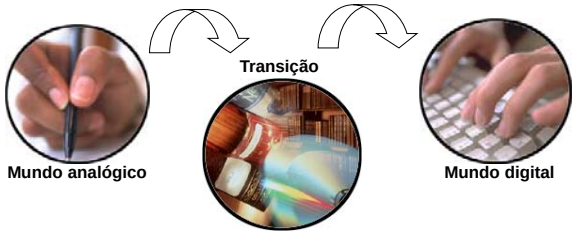
Cases

Considerações finais

2

Introdução

•Contexto



Um dos facilitadores da transição:

Assinatura, Certificação e Tempestividade digital (ACTD)

3

Porque é a ACTD um facilitador?

No caso da comprovação da idoneidade de documentos seria necessário armazenar cópia digital e original em papel;

Idoneidade de documentos ⇔ *eficácia probatória*

Três aspectos principais a tratar na ACTD:

–Aspectos Tecnológicos => envolve a área de TI;

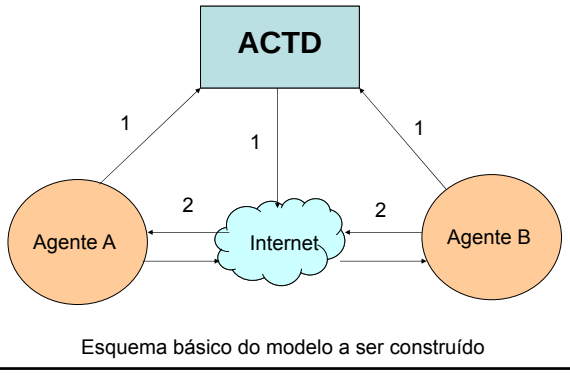
–Aspectos Jurídicos => envolve a legislação;

–Aspectos Culturais => envolve a área comportamental;

Maior barreira = área comportamental:

Estamos acostumados a lidar com papel

4

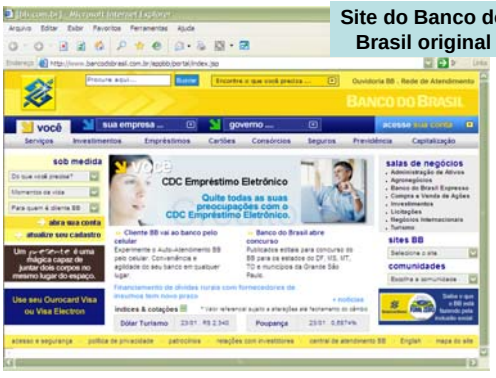


Esquema básico do modelo a ser construído

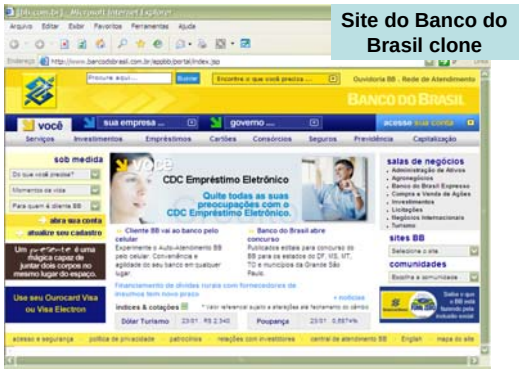
5

•Vulnerabilidades na Internet

Site do Banco do Brasil original

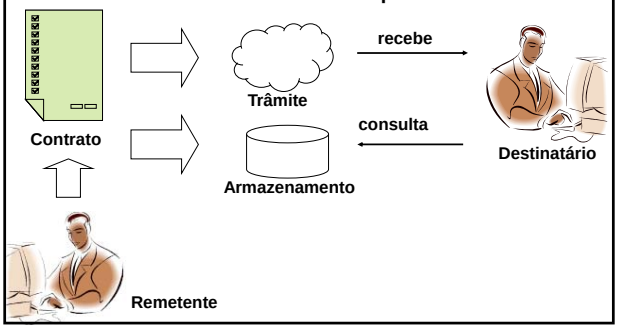


6



7

•**Vulnerabilidades em operações com documentos e processos eletrônicos**



8

Essa simples operação traz uma séria de "angústias":

Destinatário aparente = Destinatário real? => SIGILO

↑ Como se tem certeza que a mensagem não será interceptada?

Conteúdo aparente = Conteúdo real? => INTEGRIDADE

↑ Qual a garantia de que a mensagem não foi alterada?

Remetente aparente = Remetente real? => AUTENTICIDADE

↑ Como garantir que o documento é autêntico com relação ao original?

Instante aparente = Instante real? => TEMPESTIVIDADE

↑ Como se comprova que o documento foi enviado no prazo combinado?

Documento e Processo = Legal? => EFICÁCIA PROBATÓRIA

9

A ACTD atende a essas necessidades que ocorrem em função das vulnerabilidades e compreende:

Assinatura de documentos eletrônicos;

Autenticação de documentos e processos eletrônicos;

Trâmite e armazenamento de conteúdos eletrônicos com autenticidade, sigilo, integridade, legalidade, não repúdio, tempestividade e eficácia probatória.

10

Fundamentos básicos

Os fundamentos básicos para entendimento do processo são:

- Aspectos tecnológicos, jurídicos e culturais da certificação digital;
- Definição de alguns termos importantes;
- Requisitos da assinatura em documentos eletrônicos;
- Conceitos de assinatura: eletrônica, digitalizada, biométrica e digital;

11

•**Aspectos tecnológicos, jurídicos e culturais da certificação digital**

Abordam-se **aspectos tecnológicos** enfatizando:

Conhecer	➔ **Confiar** ➔	**Utilizar**
Saber o que através de leituras, cursos, etc	Ter segurança no que a tecnologia promete	Usar porque confia...

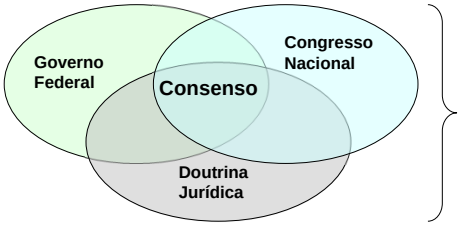
Avaliar frente as vulnerabilidades:

- •Garantias oferecidas pela tecnologia
- •Requisitos da infra-estrutura tecnológica
- •Viabilidade de aplicação com baixo custo

12

Arquivologia – Escola de Ciência da Informação
Disciplina: Introdução à Informática
GED
Prof. Mauricio Barcellos Almeida

Abordam-se **aspectos jurídicos** enfatizando:



UNCITRAL: Leis modelo das Nações Unidas

Visão abrangente = UNCITRAL

Doutrina jurídica = grandes especialistas em direito

Algumas questões na esfera do Governo e Congresso não estão resolvidas => abordar o que é consenso

13

Arquivologia – Escola de Ciência da Informação
Disciplina: Introdução à Informática
GED
Prof. Mauricio Barcellos Almeida

Abordam-se **aspectos culturais** enfatizando:

- Desigualdade social com exclusão digital;
- Falta de confiança nas promessas da tecnologia;
- Resistência à mudança de processos estabelecidos;
- Desconforto como ambiente virtual;
- Prevalência de uma cultura arraigada baseada em papel.

14

Arquivologia – Escola de Ciência da Informação
Disciplina: Introdução à Informática
GED
Prof. Mauricio Barcellos Almeida

•**Definição de alguns termos importantes**

Assinatura: marca pessoal utilizada para designar autoria;

Certificação: afirmação de certeza ou verdade;

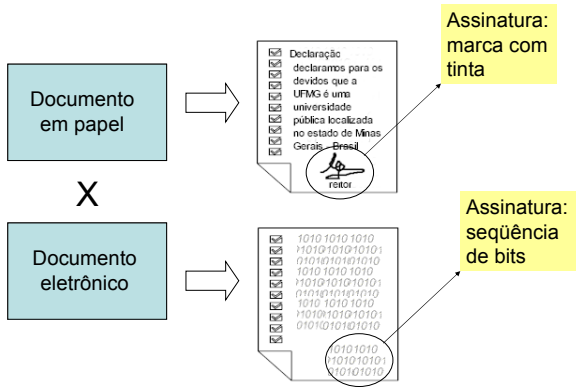
Digital: valores representados exclusivamente em números binários (em meios eletrônicos, magnéticos, ópticos, etc)

Analógico: grandezas representadas de forma contínua (pergaminho, papel, microfilme, etc);

Autenticação: ato pelo qual algo é reconhecido como verdadeiro perante a lei;

15

Escrito, original e assinatura



16

Arquivologia – Escola de Ciência da Informação
Disciplina: Introdução à Informática
GED
Prof. Mauricio Barcellos Almeida

Qual é o documento original?

No documento em papel:

- O original é papel para o qual a tinta foi transmitida; uma cópia pode ser um xerox;
- Ao fazer várias cópias, cada uma delas é diferente do original;

No documento eletrônico:

- O documento que contem os bits; uma cópia pode ser a impressão ou o que aparece na tela;
- Ao fazer várias cópias, cada uma delas é idêntica ao original pois o documento nasceu digital => todos são originais!!
- Também existem cópias eletrônicas, quando se digitaliza um documento em papel;

17

Conteúdo (mensagem)	Em papel (analógico)	Eletrônico (digital)
Escrito	Visivel (para leitura)	Acessível (sequencia de bits)
Original	Primeiro suporte	Integridade (formato original)
Assinatura	Marca pessoal em conteúdo	Autenticidade com integridade

A única barreira é não ler português

Mudança

Acessível, interpretável,mas não mais legível

18

•**Requisitos da assinatura em documentos eletrônicos**

Autenticidade:

Garantir a identificação e associação (ciente) do autor ao conteúdo; como conseqüência garante-se também o não repúdio;

Integridade

A qualquer momento poder verificar se o conteúdo assinado está integro, ou seja, invalidar a assinatura quando o conteúdo assinado for alterado (de forma similar a uma rasura em papel por exemplo);

19

Assinatura eletrônica (termo genérico)

(1)Digitalizada:

Imagem eletrônica (digitalização) da assinatura manuscrita;

É um seqüência de bits que pode se "copiada" e "colada" em quando documento;

Dessa forma não é segura para assinar documentos eletrônicos;

Não pode garantir os requisitos estabelecidos, ou seja, nem integridade nem autenticidade do documento assinado;

20

(2)Assinatura baseada em biometria

Baseada em reconhecimento de padrões: impressão digital, geometria da face, íris, voz, DNA, etc;

Usada para controle de acesso lógico: logins e senhas;

Usada para controle de acesso físico: catracas, portas, etc;

Da mesma forma que a assinatura digitalizada, a assinatura baseada em biometria é uma seqüência de bits que pode ser "copiada" e "colada" em qualquer documento;

Também não pode garantir os requisitos estabelecidos, ou seja, nem integridade nem autenticidade do documento assinado;

21

(3)Assinatura digital

Tem equivalência funcional em relação a assinatura manuscrita lavrada em papel;

Papel ↓

Conteúdo	+	Sinal do autor	=	Assinatura

Eletrônico ↓

Resumo (hash)	+	Chave do autor	=	Assinat.digital

Possibilita a qualquer momento verificar se o conteúdo assinado foi alterado (integridade);

Pode garantir a identificação do assinante (autenticidade);

22

Uma assinatura digital:

Garante uma conexão lógica entre um documento e sua respectiva assinatura (no caso do papel a conexão é física);

Utilizada para autenticação de cópias eletrônicas (documentos digitalizados) quando usada com certificação digital;

Pode garantir eficácia probatória de conteúdos e de processos eletrônicos (da mesma forma que em documentos de papel);

É o principal componente de uma ICP-Infraestrutura de Chaves Públicas;

23

ICP-Infraestrutura de Chaves Públicas

Aspectos importantes para o entendimento das ICPs

•Componentes: criptografia, função hash, assinatura digital e certificação digital (garantia de sigilo, autenticidade e integridade);

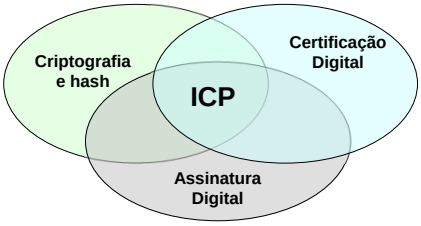
•Hierarquia, normas e padrões da ICP;

•Requisitos para garantia de resultado com a ICP;

•Modelos internacionais de ICP;

24

•Componentes: criptografia, função hash, assinatura digital e certificação digital



ICP-*Insfraestrutura de Chaves Públicas,* ou

PKI-*Public Key Infraestructure*

também conhecida como "cartório digital"

25

–Criptografia

Criptologia = cripto-análise + criptografia;

Cripto-análise = desvendar como um código foi criado, sem conhecer a regra, por força bruta;

Criptografia é tornar incompreensível;

A Criptografia oferece garantia de sigilo dos conteúdos;

Exemplo (usado no Império Romano):

Algoritmo	+	chave	=	Código criptografado
↓		↓		↓
L + D		D=3		a → d, b → e, c → f ...

A palavra "atacar" seria escrita "dxdfdu"

26

**Criptografia simétrica*

Existe uma chave única para decifrar o conteúdo eletrônico;

Rápida em relação aos outros tipos de criptografia;

Problemas:

Compartilhamento do segredo; como enviar a chave?

Multiplicidade de chaves;

27

Como resolver os problemas da criptografia simétrica?

Exercício:

Como D. João VI de Portugal poderia de comunicar através de mensagens escritas, em sigilo, com D.Pedro no Brasil, sem compartilhar segredo?

Equipamentos disponíveis: um baú e dois cadeados;

Tempo: 3 min....

28

Resposta ao exercício

D. João e D. Pedro executam os seguintes procedimentos....

1. Ao partir para Portugal, D.João leva o cadeado de D.Pedro aberto;
2. D.João coloca a mensagem para D.Pedro dentro do baú;
3. Coloca também dentro do baú o seu cadeado aberto;
4. Lacra o baú com o cadeado que trouxe aberto (cadeado de D.Pedro) e envia o baú para o Brasil;
5. D. Pedro é o único que pode abrir o baú (com sua chave) então.....

29

5. ... D.Pedro recebe o baú e abre com sua chave
6. Acessa a mensagem enviada pelo Rei;
7. Retira o cadeado do Rei (aberto);
8. Coloca no baú a mensagem resposta para D.João;
9. Coloca no baú o seu cadeado aberto (cadeado de D.Pedro);
10. Lacra o baú com cadeado do Rei (que recebeu aberto) e envia o baú para Portugal;
11. D. João recebe o baú e abre com sua chave;
12. Acessa a mensagem enviada pelo príncipe;
13. Retira o cadeado aberto do príncipe e o processo continua....

30

*Criptografia assimétrica

Tem como princípio garantir a comunicação com sigilo sem compartilhamento de segredo utilizando um par de chaves, ditas assimétricas:

Chave do cadeado = chave privada

Cadeado aberto = chave pública

Na criptografia assimétrica reside a garantia de sigilo de um documento eletrônico

31

Sigilo: apenas uma pessoa pode ter assinatura específica; o não compartilhamento de segredo através da chave privada permite o não repúdio da assinatura digital;

A autenticidade será comprovada no contexto da Certificação Digital (ver adiante); identifica-se o titular de uma assinatura pela sua chave pública correspondente;

Dessa forma, na criptografia assimétrica, considera-se:

- Um único par de chaves matematicamente relacionadas (pública e privada);
- Conteúdo cifrado por qualquer uma, só pode ser decifrado por qualquer outra;
- Segurança depende do algoritmo e tamanho da chave criptográfica, sendo recomendável respectivamente, RSA e 1024 bits

32

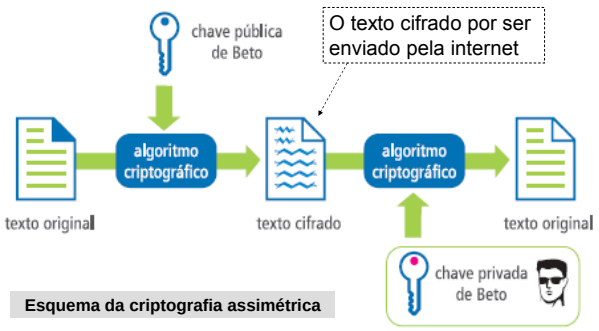
Algoritmo RSA:

Inventado em 1978 por **R**ivest, R.; **S**hamir, A.; **A**dlerman, L.

Baseia-se na dificuldade matemática de fatoração de dois números primos muito grandes;

Um *hacker*, bem treinado e equipado, por tentativa e erro demoraria cerca de 15 bilhões de anos para quebrar a chave....

33



Esquema da criptografia assimétrica

34

Premissas de confiança da criptografia assimétrica são *premissas públicas* e *premissas privadas*....

.... cada uma delas fundamentada em uma *crença sintática* e em uma *crença semântica*;

Premissa pública: o titular de um par de chaves assimétricas é conhecido por sua chave pública;

- Crença sintática: associação entre os bits que representam a chave pública e aqueles que representam o nome de seu titular é autêntica;
- Crença semântica: o nome que dá título à chave pública é o de alguém com quem se tem relação de significado;

35

Premissa Privada: o titular de um par de chaves assimétricas é quem conhece sua chave privada;

- Crença sintática: a posse e o acesso à chave primária restringe-se a quem é nomeado seu titular;
- Crença semântica: o uso autenticatório da chave privada significa declaração, por parte do titular, de sua vontade ou autoria;

36

Problemas na criptografia assimétrica:

Não é adequada para decifrar grandes volumes de dados, pois é lenta devido a sua complexidade;

Pode-se usar um sistema combinado simétrico + assimétrico;

Gera-se uma chave simétrica para ser usada em apenas uma sessão, documento ou arquivo; a parte simétrica protege o documento;

Cifra-se a chave simétrica com a chave pública do receptor e envia-se ao mesmo; a transmissão é protegida pela parte assimétrica;

Inicia-se a transmissão cifrada propriamente dita;

37

-Função Hash

O código Hash corresponde a um resumo do conteúdo eletrônico de um documento;

No código Hash cada letra do conteúdo corresponde ao seu valor numérico ASCII; a função é aplicada sobre esses valores; por exemplo H=72, O=79; J=74; E=79;

O código Hash gerado deve ser irreversível, ou seja, o documento gera o resumo, mas o resumo não gera o documento;

O código Hash deve ser resistente a colisões, ou seja, em um milhão de documentos não haverá duplicidade de resumos;

Tamanho e algoritmos recomendados: respectivamente, 128 bits; SHA-1=160 ou MD5=128;

38

Exemplo:

Na função hash reside a garantia de integridade de um documento eletrônico

Conteúdo	Função	Código
Matricula: 35 Nome: Maria Valor: 412	Num + 3	68745 (reversível, não hash)
	∑ Num	15 (hash)
	Mat+valor	**447** (hash ok)
Matricula: 21 Nome: José Valor: 534	∑ Num	15 (colisão)
	Mat+valor	**555** (hash ok)

Caso se altere o número 534 para 539 o hash passa a ser 560 ≠ 555 ➔ **Violação**

39

-Assinatura digital

O resumo Hash pode ser considerado um assinatura? Não, porque ainda falta identificar o assinante;

Componentes da Assinatura Digital:

Função Hash (resumo do documento eletrônico);

Criptografia Assimétrica (chave pública e chave privada)

Algoritmos de assinatura e verificação;

Principais padrões para assinatura digital: (necessário software)

RSA: criptografia padrão comercial;

DAS: criptografia padrão governamental;

Padrões: (necessário software)

Geração de assinatura digital;

Verificação (conferência) de assinatura digital;

40

↑ Esquema de assinatura digital

Código hash + chave privada = assinatura digital

41

Então, para produzir documentos com assinaturas digitais:

Dado um certo documento utiliza-se um função hash não reversível para produzir um código de tamanho fixo, associado de forma unívoca ao documento;

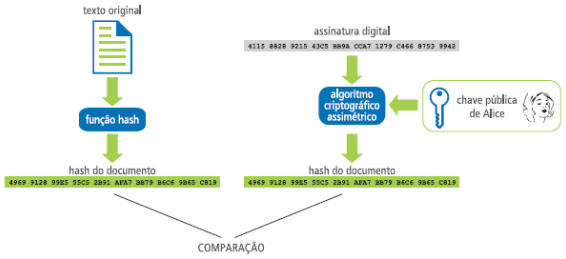
Com a chave privada de quem deseja assinar o documento, cifra-se o resumo gerado anteriormente pelo código hash;

A assinatura digital estabelece uma relação única entre o documento assinado e a pessoa que está assinando;

A verificação da assinatura se dá pela chave pública de quem assinou o documento;

Integridade é resolvida pelo Hash; identificação do assinante é atendida pela chave pública; sigilo é atendido pela chave privada

42



Esquema de conferência da assinatura

43

Algumas considerações sobre assinatura digitais:

Não torna o documento eletrônico imune a alteração, apenas logicamente imutável; caso seja alterado por hackers, pode-se perceber tal alteração;

A assinatura não é única por pessoa que assina o documento, ou seja, podem assinar diversas pessoas, desde que seus certificados digitais tenham validade;

A assinatura é única por documento, pois é gerada a partir de cada conteúdo assinado;

O par de chaves criptográficas para gerar e conferir o documento é único;

44

-Cerificação digital

A Certificação Digital é análoga a uma identidade no formato eletrônico; é o componente de confiança na Internet;

Consiste da expedição e controle da certificação por uma AC-Autoridade Certificadora;

Permite a qualquer momento atestar a titularidade de uma chave criptográfica;

A vinculação entre certificado e titular da assinatura é garantida pela AR-Autoridade de Registro;

A certificação digital é a garantia de autenticidade

45

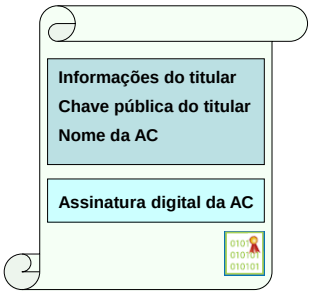
Alguns termos importantes:

Certificado digital: associação entre uma chave pública e uma pessoa ou dispositivo; deve ter prazo de validade em função da evolução da cripto-análise; sua distribuição é feita através da publicação em diretórios públicos;

AC-Autoridade Certificadora: entidade de confiança do solicitando do Certificado Digital para garantir a identidade dos envolvidos em uma operação eletrônica;

AR-Autoridade de Registro: responsável pela identificação presencial do solicitante de um Certificado Digital;

46

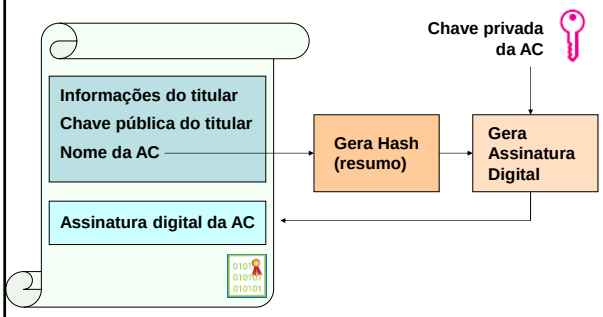


O Certificado Digital é um arquivo eletrônico que contem informações de identificação;

Permite assegurar a identidade de quem assina uma mensagem ou um documento eletrônico

Esquema de um certificado digital

47



Geração de um certificado digital
(recomendação Padrão ISO)

48

Certificado da autoridade Certificadora Raiz Brasileira

49

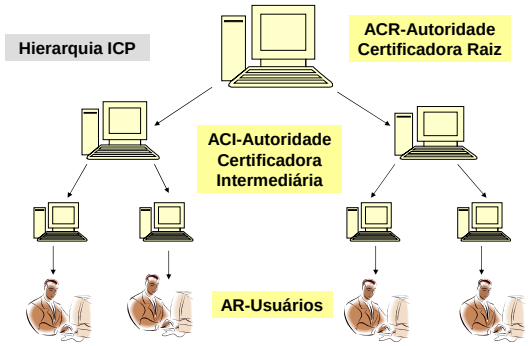
Revogação de certificados:

Um certificado deve ser revogado caso haja comprometimento da chave privada da AC ou da chave privada do titular do certificado;

A AC deve disponibilizar o OCSP-*OnLine Certificate Status Protocol* e periodicamente emitir e publicar uma lista de LCR-Certificados Revogados;

50

•**Hierarquia, normas e padrões da ICP**



51

Principais modelos de ICP:

Modelo isolado: existe uma AC-Raiz única;

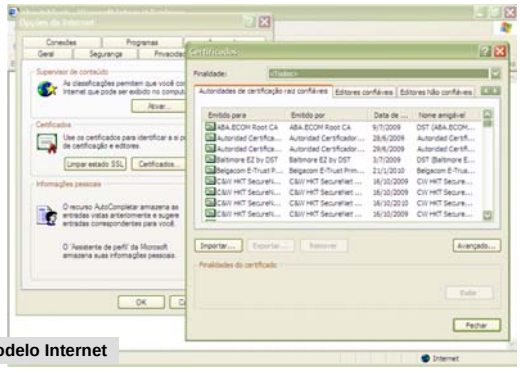
Modelo floresta: ICPs independentes com certificações cruzadas entre algumas AC-Raizes;

Modelo em malha: semelhante a floresta com certificação cruzada entre todas as AC-Raizes;

Modelo com ponte: semelhante a floresta, onde cada AC-Raiz tem certificação cruzada com uma entidade central denominada ponte (funciona como um hub);

Modelo Internet: AC-Raizes de certificados confiáveis já vem instalados no navegador;

52



Modelo Internet

53

Normas e padrões internacionais (norma ISO adotada em todo o mundo) recomendam no mínimo os seguintes documentos:

Documento de Políticas da ICP;

Declaração formal do papel de cada componente da ICP;

Responsabilidades a serem assumidas pelos usuários da ICP;

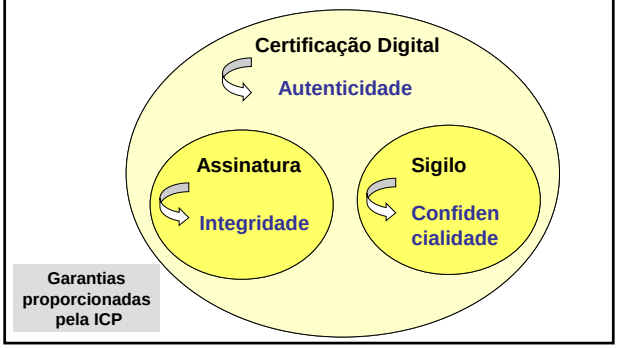
Procedimentos para manutenção de chaves;

DPC-Declaração de Práticas de Certificação;

Recomenda-se uma DPC para cada ICP;

54

•**Requisitos para garantia de resultado com a ICP**



Garantias proporcionadas pela ICP

55

Requisitos para garantias de uma ICP:

- Sistemas criptográfico seguro;
- Proteção da chave privada; (ver adiante)
- Código Hash resistente a colisões;
- Autoridade Certificadora confiável;
- Ambiente computacional adequado;

56

Níveis de proteção da chave privada:

- No *HD*: básico, não portável, sem custo;
- Em *CD*: intermediário, portável, baixo custo;
- *Smart Card*: avançado, portável, alto custo (figura)
- *Token USB*: Avançado, portável, baixo custo

***Smart card* com chave privada**

57

•**Modelos internacionais de ICP**

Modelo EuroPKI:

- Baseado na Itália e operacionalizado por universidades e instituições não governamentais;
- Adota o modelo ICP isolado;

Modelo canadense:

- De responsabilidade do governo, com o objetivo é incentivar o comércio eletrônico;
- Adota o modelo floresta com a ICP do governo funcionando como ponte;

Cont....

58

Modelo norte-americano

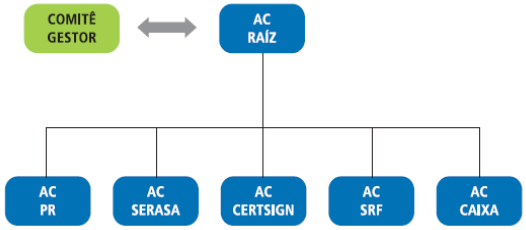
- Objetiva integrar as ICPs de agências nacionais e estaduais;
- Adota o modelo floresta, de grande porte;

Modelo Brasileiro (ICP-Brasil)

- Autoridade que define as políticas é o Comitê Gestor ligado a Casa Civil;
- Modelo isolado e hierarquizado;
- AC-Raiz fiscaliza e audita as Acs abaixo dela, mas não pode emitir certificados para usuários finais;

Cont... figura

59



Hierarquia da ICP Brasil

60

Tempestividade digital

Tempestividade ≠ temporalidade

- Temporalidade diz respeito ao período;
- Tempestividade diz respeito ao instante: poder comprovar que um evento ocorreu em data/hora regulamentada como oficial;

Considerações importantes:

- Autoridades de tempo (no Brasil o ON-Observartório Nacional);
- Sincronismo de tempo:
- Carimbo de tempo;
- Protocolos digitais
- Selo cronológico digital

Texto para leitura

61

Cases de ACTD

GOVERNO FEDERAL: o Presidente da República e Ministros têm utilizado certificados digitais na tramitação eletrônica de documentos oficiais, que serão publicados no Diário Oficial da União. Um sistema faz o controle do fluxo dos documentos de forma automática, desde a origem dos mesmos até sua publicação e arquivamento.

IMPRESSA OFICIAL DO ESTADO DE SÃO PAULO: implantou certificação digital em seu sistema que automatiza o ciclo de publicações na Internet, permitindo a eliminação das ligações interurbanas e dos congestionamentos telefônicos, uma vez que se utiliza a Internet com garantias de sigilo e privacidade, além da de garantia de autoria por parte do autor das matérias.

62

ESTADO DE PERNAMBUCO: primeiro estado brasileiro a utilizar a Certificação Digital. A Secretaria de Fazenda de Pernambuco disponibilizou um conjunto de serviços pela Internet com base na certificação digital que proporcionou diversos benefícios como: entrega de diversos documentos em uma única remessa; redução drástica no volume de erros de cálculo involuntários; apuração automática dos impostos; minimização de substituições de documentos e redução de custos de escrituração e armazenamento de livros fiscais obrigatórios.

ESTADO DO PARANÁ: projeto de grande abrangência em implantação;

INSS: projeto de grande abrangência em implantação;

63

Considerações finais

Outras aplicações da ACTD:

- Bancos, comércio, cartórios, Internet, projetos de GED, segurança ao trâmite de documentos, workflow, empresas de engenharia (plantas), receita federal, etc;

Legislação e normas de incentivo

- Existe todo um conjunto de leis e normas de órgãos que regulamenta e facilitam o uso da ACTD;

64