

# Engenharia de Segurança

Prof. Dr. Kainika Regina Lucas Jaque Castelo Branco

[Kainika@ctmc.usp.br](mailto:Kainika@ctmc.usp.br)

Slides baseados nas transparências de diversos professores e autores de livros (prof. Edward David Moreno, Márcio H. C. d'Avila, Tannenbaum, Karose, Adriano Canstian entre outros)

## Introdução aos Serviços de Segurança

Tipos de Ataque e Formas de se proteger



### Serviços de segurança

- ▶ Funcionalidades que, se presentes, possibilitam restringir determinados riscos de segurança
- ▶ Classificação:
  - Serviço de Confidencialidade
  - Serviço de Autenticação
  - Serviço de Integridade
  - Serviço de Irretratabilidade (não repudição)
  - Serviço de Disponibilidade
  - Serviço de Controle de Acesso
  - Serviço de Auditoria

3

### Serviços de Segurança

- ▶ Confidencialidade
  - Proteger uma informação armazenada ou transmitida contra divulgação às entidades não autorizadas
  - Garantir o segredo entre as comunicações de dois agentes.
  - A confidencialidade se estende inclusive em relação aos gerentes/administradores responsáveis pela segurança da rede (eles não devem ter acesso a informação que não lhes diz respeito)
  - **É objeto de política da empresa.**

4

### Serviços de Segurança

- ▶ Confidencialidade
  - **O que é spoofing ?**
  - Alguém "ouve" a sua rede através de alguma interface não protegida.
  - Em geral este é um "ataque interno" ou então realizado através de interfaces entre redes (roteador por exemplo).

7

### Serviços de Segurança

- ▶ Confidencialidade
  - Deve ser garantida desde a origem da informação através de:
    - Controle de acesso aos arquivos
    - Codificação (cifragem) das mensagens
    - Controle de acesso ao meio (rede)
  - Normalmente as violações de confidencialidade ocorrem:
    - Por acesso indevido aos arquivos
    - Por interceptação de mensagens (durante o trânsito)

5

### Serviços de Segurança

- ▶ Confidencialidade
  - Como ocorre a interceptação de mensagens em trânsito ?
    - *Spoofing*
    - Durante armazenagem intermediária
    - Por "wire-wrapping".

6

### Serviços de Segurança

- ▶ Confidencialidade
  - Como os arquivos podem ser interceptados ?
    - Em geral durante armazenagem intermediária. No caso de e-mail, temos os "mail exchangers", por exemplo.
    - Não há como garantir segurança em "MAIL EXCHANGERS"

8

### Serviços de Segurança

- ▶ Confidencialidade
  - **O que é Wire Wrapping ?**
  - Ocorre quando alguém "grampeia" sua linha de comunicações.
  - Pode ser um ataque interno ou externo
  - Em geral é difícil de ser detectado.

9

## Serviços de Segurança

### ▶ Confidencialidade

#### ▶ Como Garantir a Confidencialidade ?

- Através de mecanismos de cifragem.
- Reduzindo o número de “exchangers”
- *Impedindo o “spoofing” (intranet).*
- *Efetuando medidas nas linhas de comunicação (evitando wrapping)*

**Cifragem é a melhor garantia para a confidencialidade.**

10

## Serviços de Segurança

### ▶ Autenticidade

#### • Como Garantir Autenticidade ?

**Através dos mecanismos de autenticação!**

11

## Serviços de Segurança

### ▶ Irretratabilidade (Não repúdio)

- Garantir que uma determinada entidade ...
- que gerou uma determinada informação não possa alegar que não a tenha gerado, ou ...
- que recebeu uma determinada informação não possa alegar que não a tenha recebido.

▶ É a capacidade de provar que mensagens/dados foram realmente enviados e devidamente recebidos.

▶ Existem ataques onde forja-se o “sumiço” de mensagens/arquivos, inclusive senhas e chaves de cifragem.

16

## Serviços de Segurança

### ▶ Autenticação (Autenticidade)

- Em uma interação, possibilita comprovar a identidade de uma entidade parceira (usuário, computador, aplicação)
- Em uma mensagem, possibilita comprovar de que a mensagem foi gerada pela entidade esperada e não por uma entidade impostor

■ É a medida da “veracidade” de uma determinada informação.

■ É importante lembrar que é relativamente “fácil” fabricar informação ou adulterar informação.

11

## Serviços de Segurança

### ▶ Integridade

- Permitir determinar se um determinado recurso (armazenado ou em trânsito) foi modificado por uma entidade não autorizada

▶ É a característica que garante que a informação não tem seu conteúdo alterado durante os processos de Comunicação/Armazenamento.

**Mesmo mensagens cifradas e autenticadas podem, em determinadas circunstâncias não estar íntegras !**

14

## Serviços de Segurança

### ▶ Irretratabilidade (Não repúdio)

- Todas as mensagens válidas devem ser aceitas e deve ser possível confirmar quem originou a mensagem e quando ela foi recebida.

17

## Serviços de Segurança

### ▶ Autenticidade

#### • Como uma informação pode ser fabricada ?

- A partir do conhecimento de dados:
- E-mail/Identificações
- Interceptação de comunicações

**Mesmo uma mensagem encriptada (cifrada) pode ser falsa ou adulterada!**

12

## Serviços de Segurança

### ▶ Integridade

- Mensagens não devem ser “embaralhadas”
- Mensagens não devem ser “duplicadas”
- Mensagens não devem ser alteradas.

- Por modificação de conteúdo existente
- Por inserção de conteúdo
- Por deleção de conteúdo

15

## Serviços de Segurança

### ▶ Disponibilidade

- Garantir que um determinado recurso (serviço de rede, aplicação, meio de comunicação, arquivo, ...) esteja sempre “disponível” para as entidades autorizadas

▶ Os serviços devem ser disponíveis continuamente segundo o disposto pela gerência/Administração da rede.

▶ Ou seja, nos períodos e nos regimes especificados, os serviços especificados devem ser disponíveis.

18

## Serviços de Segurança

- ▶ **Disponibilidade**
- ▶ Quais os ataques mais frequentes em relação à disponibilidade ?
- Ataques que degradam os serviços
- Ataques que interrompem os serviços

19

## Serviços de Segurança

- ▶ **Disponibilidade**
- ▶ Exemplos de ataques envolvendo a redução de disponibilidade:
  - *Denial of Service (Dos)*
  - "Pingão"
  - *Mail Bombs*

22

## Serviços de Segurança

- ▶ **Controle de Acesso Envolve**
- ▶ Além de características:
  - "espaciais" (host, serviços e redes que podem ser usados por um usuário ou por grupos de usuários) temos as
  - características "temporais" (quando os recursos podem ser usados) e as
  - características "volumétricas" (qual a quantidade de recursos disponíveis para cada usuário/grupo de usuários).

25

## Serviços de Segurança

- ▶ **Disponibilidade**
- ▶ Como funcionam os ataques que degradam os serviços ?
- Por excesso de solicitações
- Pela ausência de confirmações
- Por induzir à operação incomum

20

## Serviços de Segurança

- ▶ **Controle de Acesso**
- Garantir que somente entidades autorizadas consigam acesso a um determinado recurso
- Garantir que autorizações de acesso a um determinado recurso sejam dadas apenas pelos responsáveis e não sejam alteradas indevidamente
- ▶ Deve ser possível controlar o acesso às informações.
- ▶ Por controlar o acesso se entende:
  - Definir explicitamente permissões
  - Auditorar os acessos.

23

## Serviços de Segurança

- ▶ **Controle de Acesso**
- ▶ Também define-se no controle de acesso o MODO pelo qual os usuários/grupos de usuários utilizam os recursos do sistema:
  - de forma ativa: (Ex. ON LINE)
  - de forma passiva: (Ex. "Call back")

26

## Serviços de Segurança

- ▶ **Disponibilidade**
- ▶ Como funcionam os ataques que interrompem os serviços ?
- Por ocupação completa da banda de comunicação
- Induzindo aplicações ao erro
- Gerando alarmes (induzindo o sistema a acreditar que a segurança foi violada).

21

## Serviços de Segurança

- ▶ **Controle de Acesso Envolve**
- ▶ Acesso a programas e serviços em "hosts"
- ▶ Acesso às redes
- ▶ Autenticar/legitimar usuários
- ▶ Controlar privilégios "por usuário"

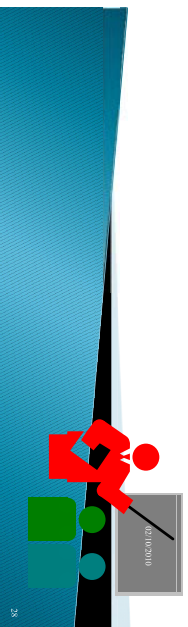
24

## Serviços de Segurança

- ▶ Auditoria
- Armazenamento de informações sobre utilização de recursos do sistema

27

## Como podem ser os Ataques ?



30

### Ataques: Passivos e/ou Ativos

- ▶ **Ataques Passivos:** o atacante não interfere na operação normal do sistema. Em geral, ele capta comunicações durante o trânsito destas pela rede.
- ▶ **Ataques Ativos:** o atacante interfere na operação normal do sistema, tanto através da utilização indevida de serviços/recursos quanto pela interferência em serviços.

30

### Ataques Passivos

- ▶ São difíceis de detectar. Usualmente os usuários reclamam de "vazamento" de informações.
- ▶ Envolvem o roubo de conteúdo (dados)
- ▶ Envolvem "espionagem" em relação a uma topologia de rede/análise de serviços, etc..

30

### Como evitar Ataques Passivos ?

- ▶ Utilizando cabeamento óptico
- ▶ Utilizando analisadores de continuidade
- ▶ Configurando corretamente equipamentos de rede
- ▶ Implementando **"FIREWALLS"**.

31

### Ataques Ativos ?

- ▶ Envolvem a ação direta do intruso sobre um conjunto de sistemas.
- ▶ Quanto à natureza podemos ter:
  - Ataques à disponibilidade
  - Ataques à integridade
  - Ataques à autenticidade

32

### Ataques Ativos – Disponibilidade

- ▶ Em geral visam a interrupção ou a degradação sensível de desempenho de algum serviço.
- ▶ Podem ser feitos por consumo excessivo de recursos (e-mail gigante, acesso histórico à serviços, etc..)
- ▶ podemos utilizar características de serviços para interrompê-los (*Denial of Service*).

33

### Ataques Ativos – Integridade

- ▶ Visam a alteração/destruição de conteúdos armazenados em um sistema.
- ▶ Por alteração entende-se também inserção de conteúdos (programas por exemplo).
- ▶ Em geral são efetuados através do acesso a serviços disponíveis e não devidamente configurados/protegidos (e-mail, FTP, HTTP, ...) e, atualmente JAVA.

34

### Ataques Ativos – Integridade (2)

- ▶ Ataques ativos podem estar associados à ataques passivos anteriores: alguém "grava" transações através da rede e usa os **"usercodes"** e **"passwords"** obtidos para ganhar acesso ilegal ao sistema.

35

### Ataques Ativos – Autenticidade

- ▶ Envolvem a geração de conteúdos falsos (apócrifos).
- ▶ Em geral são ataques que afetam serviços de mensagens (e-mail, transações ON-LINE (inclusive SQL), HTTP Forms, etc..)
- ▶ Em geral estão associados à ataques passivos ocorridos anteriormente.

36

## Como evitar ataques ?

- ▶ Mantendo uma equipe de trabalho confiável e organizada;
- ▶ Mantendo procedimentos rígidos de trabalho;
- ▶ Mantendo registro auditável de todas as ações efetuadas sobre os sistemas e redes
- ▶ Mantendo instalações seguras (físicas e logicamente).

37

## Como Proceder num Ataque ?

- ▶ Interromper o serviço atacado.
- ▶ Auditar o sistema visando descobrir:
  - Quem fez a proeza
  - Quando a proeza foi feita
  - Onde (a partir de onde) a proeza foi feita
  - Como o ataque foi feito
  - Por quê (qual o objetivo do ataque)

38

## Como Proceder num Ataque ? (4)

- ▶ Jamais procurar ocultar o fato se houver vítima identificável.
- ▶ Segundo Jurisprudência que está sendo firmada, isso pode caracterizar até delito doloso (especialmente nos casos comerciais/industriais).

39

## Como evitar ataques ? (2)

- ▶ Auditar o sistema periodicamente, procurando verificar flutuações no desempenho (Ex. a rede cai de vez em quando ...) e situações anormais 9EX. E-mails estranhos, recusas repetidas em conexões FTP, etc..)
- ▶ Auditar os usuários/clientes
- ▶ Assinar os serviços de notificação de ataques, "bugs" de software, etc..
- ▶ Corrigir imediatamente os "bugs" de software que forem notificados.

38

## Como Proceder num Ataque ? (2)

- ▶ Notificar os organismos competentes:
  - À FAPESP (em São Paulo)
  - À RNP através de seus POPS
  - O Provedor donde partiu o ataque
  - A vítima do ataque
- ▶ Se pertinente efetuar boletim de ocorrência em delegacia de policia.

41

## Como evitar ataques ? (3)

- ▶ Não descuidar da verificação de senhas e permissões de acesso.
- ▶ Estabelecer mecanismos de envelhecimento de senhas.
- ▶ Nunca manter usuários "zombies": Ex funcionários e ex clientes
  - devem ter TODAS as senhas invalidadas
- ▶ Nunca manter contas coletivas: Guest/anonymous, etc.. Devem ser fiscalizados assiduamente.
- ▶ Ser severo com usuários indisciplinados.
- ▶ **JAMAIS TRANSIGIR EM RELAÇÃO ÀS NORMAS DE SEGURANÇA.**

39

## Como Proceder num Ataque ? (3)

- ▶ Alterar/Corrigir o sistema de forma que o ataque não seja mais possível.
- ▶ Informar os demais provedores (em termos convenientes, é claro), o ocorrido. Se for identificado um "agente", notificar CLARAMENTE a identidade do agente (nome, endereço, etc..)

42

## Infra-estrutura de Chave Pública no Brasil

### Agenda

- ▶ O que é o ICP-Brasil ?
- ▶ Histórico da Regulamentação
- ▶ Estudo de Caso SPB



44

## Conceitos

- ▶ O que é o ICP Brasil ?
  - Trata-se de um conjunto de técnicas, práticas e procedimentos a ser implementado pelas organizações governamentais e privadas brasileiras com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública.

45

# Histórico da Regulamentação

**DECRETO Nº 3.505, DE 13 DE JUNHO DE 2000.**

- ▶ Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
- ▶ Fica instituído o Comitê Gestor da Segurança da Informação coordenado pelo **Gabinete de Segurança Institucional da Presidência da República** e formado por representantes de:
  - Ministério das Relações Exteriores;
  - Ministério da Saúde;
  - Ministério do Desenvolvimento, Indústria e Comércio Exterior;
  - Ministério do Planejamento, Orçamento e Gestão;
  - Ministério das Comunicações;
  - Ministério da Ciência e Tecnologia;
  - Casa Civil da Presidência da República
- Ministério da Justiça;
- Ministério da Defesa;
- Ministério da Fazenda;

46

# Histórico da Regulamentação

**DECRETO Nº 3.587, DE 5 DE SETEMBRO DE 2000.**

- ▶ Atribuições da ACP:
  - VI – definir regras operacionais e normas relativas a:
    - a) Autoridade Certificadora – AC;
    - b) Autoridade de Registro – AR;
    - c) assinatura digital;
    - d) segurança criptográfica;
    - e) repositório de certificados;
    - f) renovação de certificados e cópia de segurança e recuperação de chaves;
    - g) atualização automática de chaves;
    - h) histórico de chaves;
    - i) certificação cruzada;
    - j) suporte a sistema para garantia de irretroatividade de transações ou de operações eletrônicas;
    - k) período de validade de certificado;
    - l) aplicações cliente;

46

# Histórico da Regulamentação

**MEDIDA PROVISÓRIA Nº 2.200-2, DE 24 DE AGOSTO DE 2001.**

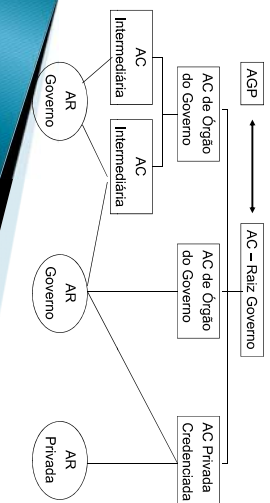
- ▶ Institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências
- DECRETO Nº 3.996, DE 31 DE OUTUBRO DE 2001.**
- ▶ Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

52

# Histórico da Regulamentação

**DECRETO Nº 3.587, DE 5 DE SETEMBRO DE 2000.**

- ▶ Estabelece normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal – ICP-Gov, e dá outras providências
- Arquitetura do ICP-Gov**



47

# Histórico da Regulamentação

**DECRETO Nº 3.587, DE 5 DE SETEMBRO DE 2000.**

- ▶ Atribuições da Autoridade de Gestão de Políticas:
  - I – propor a criação da Autoridade Certificadora Raiz – AC Raiz;
  - II – estabelecer e administrar as políticas a serem seguidas pelas AC;
  - III – aprovar acordo de certificação cruzada e mapeamento de políticas entre a ICP-Gov e outras ICP externas;
  - IV – estabelecer critérios para credenciamento das AC e das Autoridades de Registro – AR;
  - V – definir a periodicidade de auditoria nas AC e AR e as sanções pelo descumprimento de normas por ela estabelecidas;

48

# Histórico da Regulamentação

**DECRETO Nº 3.587, DE 5 DE SETEMBRO DE 2000.**

- ▶ Atribuições da ACP:
  - VII – atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Gov, em especial da Política de Certificados – PC e das Práticas e Regras de Operação da Autoridade Certificadora, de modo a garantir:
    - a) atendimento às necessidades dos órgãos e das entidades da Administração Pública Federal;
    - b) conformidade com as políticas de segurança definidas pelo órgão executor da ICP-Gov; e
    - c) atualização tecnológica.

46

# Histórico da Regulamentação

**DECRETO Nº 3.872, DE 18 DE JULHO DE 2001**

- ▶ Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira – CC ICP-Brasil, sua Secretaria-Executiva, sua Comissão Técnica Executiva e dá outras providências.

51

# Histórico da Regulamentação

**RESOLUÇÃO Nº 1, DE 25 DE SETEMBRO DE 2001.**

- ▶ Aprova a Declaração de Práticas de Certificação (DPC) da AC-Raiz da ICP-Brasil

**RESOLUÇÃO Nº 2, DE 25 DE SETEMBRO DE 2001.**

- ▶ Aprova a Política de Segurança da ICP-Brasil.

**RESOLUÇÃO Nº 3, DE 25 DE SETEMBRO DE 2001**

- ▶ Resolve designar a seguinte Comissão para auditar a Autoridade Certificadora Raiz – AC Raiz e seus prestadores de serviços

53

# Histórico da Regulamentação

**RESOLUÇÃO Nº 4, DE 22 DE NOVEMBRO DE 2001.**

- ▶ Altera a Declaração de Práticas de Certificação da AC Raiz da ICP-Brasil

**RESOLUÇÃO Nº 5, DE 22 DE NOVEMBRO DE 2001**

- ▶ Aprova o relatório de auditoria da AC Raiz.

54

## Histórico da Regulamentação

### RESOLUÇÃO Nº 6, DE 22 DE NOVEMBRO DE 2001.

- ▶ Aprova os critérios e procedimentos de credenciamento das entidades integrantes da ICP-Brasil.
- a) Ser órgão ou entidade de direito público ou pessoa jurídica de direito privado;
- b) Estar quite com todas as obrigações tributárias e os encargos sociais instituídos por lei;
- c) Atender aos requisitos relativos à qualificação econômico-financeira estabelecidos, conforme a atividade a ser desenvolvida, nos anexos IV, V e VI; e
- d) Atender às diretrizes e normas técnicas da ICP-Brasil relativas à qualificação técnica, constantes dos documentos relacionados no Anexo IV, aplicáveis aos serviços a serem prestados.

55

## Histórico da Regulamentação

### RESOLUÇÃO Nº 7, de 12 de Dezembro de 2001.

- ▶ Aprova os requisitos mínimos para políticas de certificado na ICP-Brasil

### RESOLUÇÃO Nº 8, de 12 de Dezembro de 2001.

- ▶ Aprova os requisitos mínimos para as declarações de práticas de certificação das autoridades certificadoras da ICP-Brasil

### RESOLUÇÃO Nº 9, DE 12 DE DEZEMBRO DE 2001.

- ▶ Estabelece regras transitórias para a ICP-Brasil

56

## Histórico da Regulamentação

### PORTARIA Nº 1, DE 12 DE DEZEMBRO DE 2001.

Comunicado de geração das chaves assimétricas e do certificado digital da Autoridade Certificadora Raiz da ICP-Brasil



57

## Histórico da Regulamentação

### RESOLUÇÃO Nº 10, DE 14 DE FEVEREIRO DE 2002.

- ▶ Estabelece as diretrizes da política tarifária da Autoridade Certificadora Raiz - AC Raiz da ICP-Brasil

Art. 2º As tarifas cobradas em virtude da prestação do serviço de emissão de certificados de que trata o art. 1º podem variar, na forma definida previamente em ato normativo da AC Raiz, entre R\$ 1.000.000,00 (cem mil reais) e R\$ 500.000,00 (quinhentos mil reais), em razão:

- I - do seu prazo de validade; e
- II - dos tipos de certificados a serem emitidos pela AC a ser credenciada.

58

## Histórico da Regulamentação

### RESOLUÇÃO Nº 11, DE 14 DE FEVEREIRO DE 2002

- ▶ Altera os requisitos mínimos para as políticas de certificado na ICP-Brasil, a declaração de práticas de certificação da AC Raiz da ICP-Brasil, delega atribuições para a AC Raiz e dá outras providências

### RESOLUÇÃO Nº 12, DE 14 DE FEVEREIRO DE 2002

- ▶ Estabelece regras processuais para credenciamento na ICP-Brasil.

59

## Estudo de Caso

### Reestruturação do Sistema de Pagamentos Brasileiro

02/10/2011

60

## Objetivo da Reestruturação

- ▶ Redução do Risco Sistemico
- ▶ Hoje o Banco Central é refém do risco sistemico
- ▶ Em caso de quebra de banco no mercado financeiro o BACEN deve assumir o prejuízo.
- ▶ Aumentar a eficiência dos instrumentos de pagamento
- ▶ Estimular a concorrência no mercado financeiro

61

## Problemas do Sistema Atual

- ▶ Atualmente, mesmo que o banco não possua saldo suficiente para satisfazer os pagamentos previstos às 7:00 hrs, o Banco Central permite a liquidação e o banco passa a ter o seu saldo negativo na Conta Reserva.
- ▶ Este saldo negativo é, normalmente, regularizado às 23:00 hrs com as negociações dos títulos públicos.
- ▶ Em média, a soma dos saldos negativos dos bancos atinge R\$ 6 bilhões.
- ▶ Essa é a dimensão do risco que a sociedade brasileira assume por intermédio do Banco Central.

62

## Problemas do Sistema Atual

- ▶ Quando um banco apresenta problemas de liquidez, o Banco Central poderia **não** permitir que o seu saldo ficasse negativo entre as 7:00 e 23:00 hrs.
- ▶ Porém, se fizesse isso, estaria transferindo o problema de liquidez do banco para todo o resto do mercado financeiro e clientela do sistema financeiro.
- ▶ Isto poderia criar uma crise sistêmica, com a quebra sucessiva de diversos bancos (feito domíno).

63

## Problemas do Sistema Atual

### ▶ Conclusão:

- O Banco Central assume o risco das transações cujas instituições operam com saldo negativo na Conta Reserva.

64

## Soluções

▶ O novo SPB compreende um conjunto de medidas que procuram solucionar os graves problemas de risco sistêmico e responsabilidade concentrada no Banco Central:

- Monitoramento em **tempo real** do saldo das Contas Reserva, **não sendo permitido saldo devedor** em qualquer momento;
- Infra-estrutura de comunicação nova e dedicada às operações do mercado financeiro nacional, garantindo transações em tempo real com segurança e confiabilidade.
- Transfêrencia do risco do mercado financeiro privado para o próprio mercado financeiro privado, através da adoção de regras mais rígidas e mecanismos de gerenciamento de risco.

65

## Tecnologia adotada para Segurança do Sistema

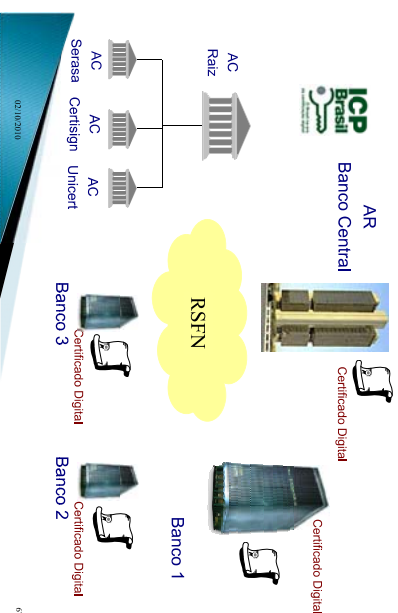
▶ Todas as mensagens transmitidas e recebidas devem ser ou estar:

- Assinadas Digitalmente pelo Emissor
- Criptografadas com uma chave aleatória
- Chave aleatória (simétrica) criptografada com a chave pública do receptor

62/10/2010

66

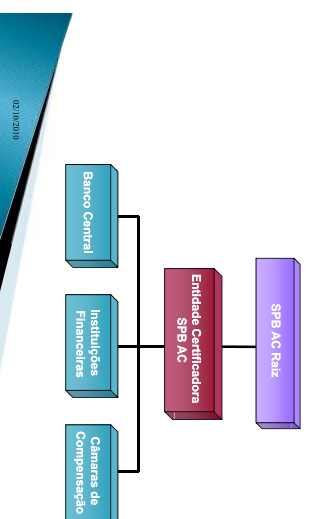
## Arquitetura do Sistema



67

## Arquitetura do Sistema

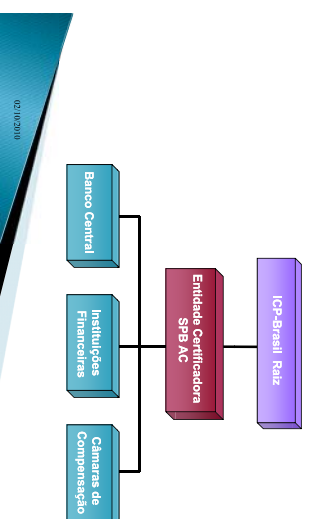
### Hierarquia Atual de Certificação



68

## Arquitetura do Sistema

### Hierarquia Proposta de Certificação (ICP-Brasil)



69

## RESUMO

62/10/2010

70

## Criptografia – Serviços Oferecidos

Serviços	Descrição
Disponibilidade	Garante que uma informação estará disponível para acesso no momento desejado.
Integridade	Garante que o conteúdo da mensagem não foi alterado.
Controle de acesso	Garante que o conteúdo da mensagem será acessado somente por pessoas autorizadas.
Autenticidade da origem	Garante a identidade de quem está enviando a mensagem.
Não-repudição	Previne que alguém negue o envio e/ou recebimento de uma mensagem.
Privacidade (confidencialidade ou sigilo)	Impede que pessoas não autorizadas tenham acesso ao conteúdo da mensagem, garantindo que apenas a origem e o destino tenham conhecimento.

62/10/2010

71

## Serviços Oferecidos

Exemplo de aplicação: Compra pela Internet

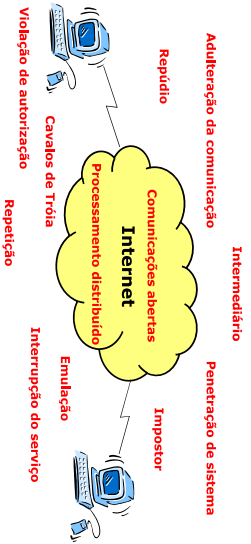
- Informação que permite a transação - valor e descrição do produto adquirido - precisa estar disponível no dia e na hora que o cliente deseja utilizá-la (**disponibilidade**).
- O valor da transação não pode ser alterado (**integridade**).
- Somente o cliente que está comprando e o comerciante devem ter acesso à transação (**controle de acesso**).
- O cliente que está comprando deve ser quem diz ser (**autenticidade**).
- O cliente tem como provar o pagamento e o comerciante não tem como negar o recebimento (**não-repúdio**).
- O conhecimento do conteúdo da transação fica restrito aos envolvidos (**privacidade**).

62/10/2010

72



## Ameaças do Ambiente Eletrônico



73

## Assuntos de Interesse

- algoritmos e técnicas criptográficas
  - aspectos legais da segurança
  - auditoria e análise em sistemas
  - avaliação da segurança
  - biometria e sistemas biométricos
  - certificação de sistemas e de software
  - comércio eletrônico
  - criminalística computacional
  - dispositivos móveis, sistemas embarcados e redes sem fio
  - hardware criptográfico, RFID, cartões inteligentes
  - infra-estrutura de chaves públicas
  - integridade e confiabilidade da informação
  - medidas e sistemas de contingência face a desastres
  - modelos e técnicas de autenticação
  - modelos e técnicas de controle de acesso
  - multimídia distribuída e TV digital

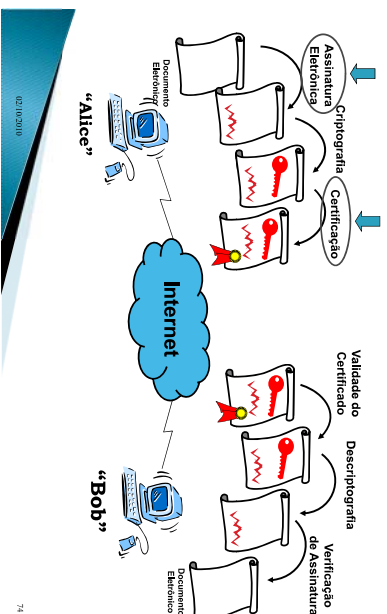
76

## Lista de Exercícios

1. Explique as 3 principais conclusões sobre as ameaças à segurança (Humana, Endógena, Gerência Relapsa)
2. Explique a importância de se estabelecer:
  - Ambiente "saúdável" da equipe
  - políticas de segurança
3. Quais os 7 serviços de segurança
  - Qual deles é o mais importante
4. O que é o ICP-Brasil (Infra-estrutura de Chave Pública). Qual a importância desse projeto ?

79

## Comunicação Segura



74

## Assuntos de Interesse

- padronização e normalização
  - pirataria de software
  - políticas de segurança
  - protocolos de segurança
  - segurança adaptativa
  - segurança em grades computacionais, redes P2P e redes overlay
  - segurança em middleware (Java RMI, JZEE, CorbaSec, Net, etc.)
  - segurança em redes
  - segurança em serviços web (WS-Security, SOAP, XML, XACML, etc.)
  - segurança em sistemas distribuídos
  - segurança em sistemas operacionais
  - técnicas para desenvolvimento de sistemas seguro

77

## Engenharia de Segurança

Prof.<sup>a</sup> Dr.<sup>a</sup> Kalinka Regina Lucas Jaquie Castelo Branco  
[kalinka@icmc.usp.br](mailto:kalinka@icmc.usp.br)

Slides baseados nas transparências de diversos professores e autores de livros  
(prof. Edward David Moreno, Marcio H. C. d'Ávila, Tamboum, Kurose, Adriano Canstian entre outros)

## Criptografia Simétrica x Assimétrica

### Assinatura Digital

- Qual a melhor técnica?
- Como garantir a autenticidade de quem envia a mensagem?
- Como garantir a integridade do conteúdo?

### Certificado Digital

75

## Assuntos de Interesse

- Tecnologias de 'firewall'
  - tolerância a intrusões
  - votação eletrônica
  - vírus, 'worms' e outros códigos nocivos
  - vulnerabilidades, ataques e detecção de intrusões

78