INE 6202 - Informática Médica

EGC 9001 - Informática e Modelagem de Conhecimento Aplicados à Saúde

Transformando Dados Clínicos em Computador em Documentos Médicos Válidos:

Segurança, Criptografia e Protocolização digital de documentos eletrônicos

Estrutura da apresentação

- 1. Fundamentos
  - Requisitos juridicamente necessários
  - Tripé Tecnológico da Segurança
  - Estudo e implementações
  - Auditoria
  - Sincronização de relógios
- 2. Prática
  - O que é oferecido pelo mercado
- 3. Requisitos
  - FDA e SBIS

MSOffice1 P. tal, etc
; 30/4/2005

Idéia geral

- Avanço da informática: transações eletrônicas
  - Papel -> documentos eletrônicos
  - Mudança no conceito de documento
- Tecnicamente e juridicamente seguros:
  - Datados e assinados digitalmente
  - Transmitidos de forma segura e com garantia de sigilo de dados sensíveis

MSOffice2 Protocolacao Digital de Doc. Ele.

1.Introducao

; 1/5/2005

Requisitos mínimos juridicamente necessários

- Autenticidade
- Integridade
- Irrefutabilidade
- Tempestividade

A VALIDADE JURÍDICA DOS DOCUMENTOS DIGITAIS

João Agnaldo Donizete Gandini
Juiz de Direito em Ribeirão Preto (SP), mestrando pela Unesp, professor da Faculdade de Direito da Universidade de Ribeirão Preto

Diana Paola da Silva Salomão
Advogada em Ribeirão Preto (SP)

Cristiane Jacob
Acadêmica de Direito pela Universidade de Ribeirão Preto

Artigo escrito em Mai/2002 e
inserido neste site em Nov/2002

Sumário: **1. Introdução. 2. O documento digital. 2.1 Conceito de documento digital. 2.2 Evolução do documento digital. 3. As condições básicas para o alcance da validade jurídica dos documentos digitais. 4. Arquivos digitais como instrumento e meio de prova. 5. As vantagens e desvantagens do uso dos documentos digitais. 6. O tratamento legislativo em outros países. 7. A regulamentação dos documentos digitais no Brasil. 8. Considerações finais.**

---

1. Introdução

O presente trabalho tem por finalidade analisar a possibilidade de atribuirmos validade jurídica aos documentos digitais.

Dentre as diversas questões em torno da informática jurídica, entamos por

Autenticidade

- Autêntico:

1. Que é do autor a quem se atribui.
2. A que se pode dar fé; fidedigno:
3. Que faz fé:
4. Legalizado, autenticado.
5. Verdadeiro, real:
6. Genuíno legítimo, lídimo:

Integridade

- Íntegro:

1. Inteiro, completo.
2. Perfeito, exato.
3. Reto, imparcial, inatacável.

Irrefutabilidade

- Irrefutável

1. Evidente, irrecusável, incontestável.

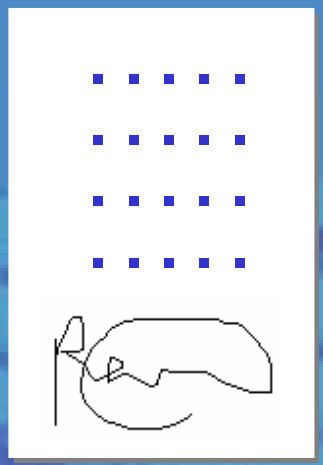
Tempestividade

- *Aurelio*: Que vem ou sucede no tempo devido; oportuno.
- *Houaiss*: oportunidade, no tempo próprio, o que ocorre no momento certo, oportuno no tempo devido

- Possibilidade de comprovar que um evento eletrônico ocorreu em um determinado instante.

Papel x documento eletrônico

Papel



10101010
10101010
10101010
10101010

10101010
10101010

Eletrônico

Visualizador

Sistema de Assinatura

Atributos de um documento eletrônico confiável

- **Autenticidade** – Certeza e Formalidade da Autoria
- **Integridade** – Certeza e inalterabilidade do Conteúdo
- **Confidencialidade**
  Sigilo

  Possibilidade de restringir o acesso ao conteúdo
- **Irretratabilidade**
  Irrefutabilidade

  Não-repúdio
- **Tempestividade**
  Irretroatividade

  Certeza e **Imparcialidade** quanto à:
  - **Quando** um documento foi criado
  - **Relação de precedência**

Estrutura da Segurança na Internet

Outros requisitos

- Autoridade Certificadora
- Plataforma computacional
  - Protocolação
  - Transmissão
  - Assinatura
- Informação temporal

MSOffice3 Protocolacao Digital de Doc. Ele.

1.Introducao

; 1/5/2005

Confidencialidade e Sigilo: Acesso Seguro

- Para que dados/documentos possam trafegar na Internet sem que outro os intercepte e veja seu conteúdo é necessário esconder esse conteúdo
  - > Criptografia
  - do grego “escrita secreta” - *kryptós gráphein* é a ciência de reescrever um texto de forma a esconder o seu significado

Criptografia

- 2 principais tipos:
  - Código
    - Utiliza substituição de palavras de acordo com um códice.
      - Ex: general <-> banana,
        matar <-> comer,
        inimigo <-> macaco
        O macaco comeu a banana = O inimigo matou o general
  - Cifra
    - Utiliza substituição, adição, subtração de símbolos da linguagem de acordo com uma regra
      - torna a mensagem ilegível
      - Ex.: “língua do Pê”
      - pode usar um parâmetro: chave de encriptação

Criptografia

- Cifra:
  - importância na criptografia digital
    - grandes quantidades de texto cifrado podem ser geradas automaticamente
  - algoritmo (método) + chave (parâmetro) geram mensagem cifrada (criptografada)
    - vantagem: chave pode ser variada
- 2 tipos:
  - chave simétrica
    - a chave usada para codificar é a mesma para decodiifcar
    - se eu descubro a chave posso não só conhecer o conteúdo das mensagens como enviar mensagens falsas
  - chave assimétrica
    - a chave para decodificar é diferente da usada para codificar

Criptografia de Chave Simétrica

- Usa a mesma chave para cifrar e decifrar.
- Vantagem: Algoritmos simples e rápidos
  - usada desde a antigüidade
  - versão moderna inventada entre 1972-76 nos EUA
  - algoritmo mais conhecido: Data Encryption Standard (DES).
- Desvantagem:
  - de alguma forma os dois lados tem de conhecer a chave
  - riscos
    - usava-se carros fortes para transportar envelopes com chaves entre bancos para troca regular das chaves
    - !! se eu conheço a chave posso gerar mensagens falsas

Criptografia de Chave Simétrica

Bastão cifrador Scítala

```
 _____________________________________
|   |   |   |   |   |   |   |
|   | H | E | L | P | M |   |
|___| E | I | A | M | U |___|
    | N | D | E | R | A |   |
    | T | T | A | C | K |   |
    |   |   |   |   |   |   |
 _____________________________________
HELP ME I AM UNDER ATTACK
```

Máquina Cifradora Enigma

Criptografia de Chave Assimétrica

- A chave usada para decriptar não é a mesma que foi usada para encriptar
- Padrão: métodos de pares de chave pública/privada: criptografia de chave pública
  - cada participante possue duas chaves: uma pública e outra privada
    - a pública eu publico para todos terem, a privada é só minha
  - a chave pública é resultado de uma operação matemática sobre a chave privada
  - para mandar uma mensagem para João, eu uso a minha chave privada e a chave pública de João para encriptar uma mensagem para ele
  - João para decriptar a mensagem utiliza a sua chave privada e minha chave pública

Criptografia de Chave Assimétrica: RSA

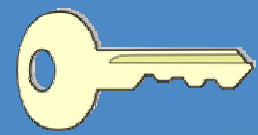
11101011100001010101010101010101010.... 1 número primo muito grande

+

11101011100001010101010101010101010.... outro número primo muito grande

=

11101011100001010101010101010101010.... fazem uma chave privada



multiplico esses dois números primos muito grandes entre si:

11101011100001010101010101010101010.... x **11101011100001010101010101010101010....**

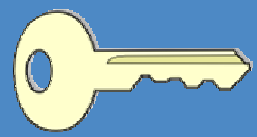
obtenho a chave pública:

11101011100100011111110101010101101010110101010101110001010101010101010101010....

Encriptando com Chave Assimétrica: RSA

11101011100100011111110101010101101010110101010101110001010101010101010101010....

a chave pública de **João**



...encripta um documento só para os olhos de João pois....

...João vai usar para decifrar....

11101011100001010101010101010101010....

11101011100001010101010101010101010....

a chave privada **dele**

Confidencialidade e Sigilo: Acesso Seguro

- Transferência encriptada de dados na Web utiliza o protocolo SSL/TLS - Secure Socket Layer

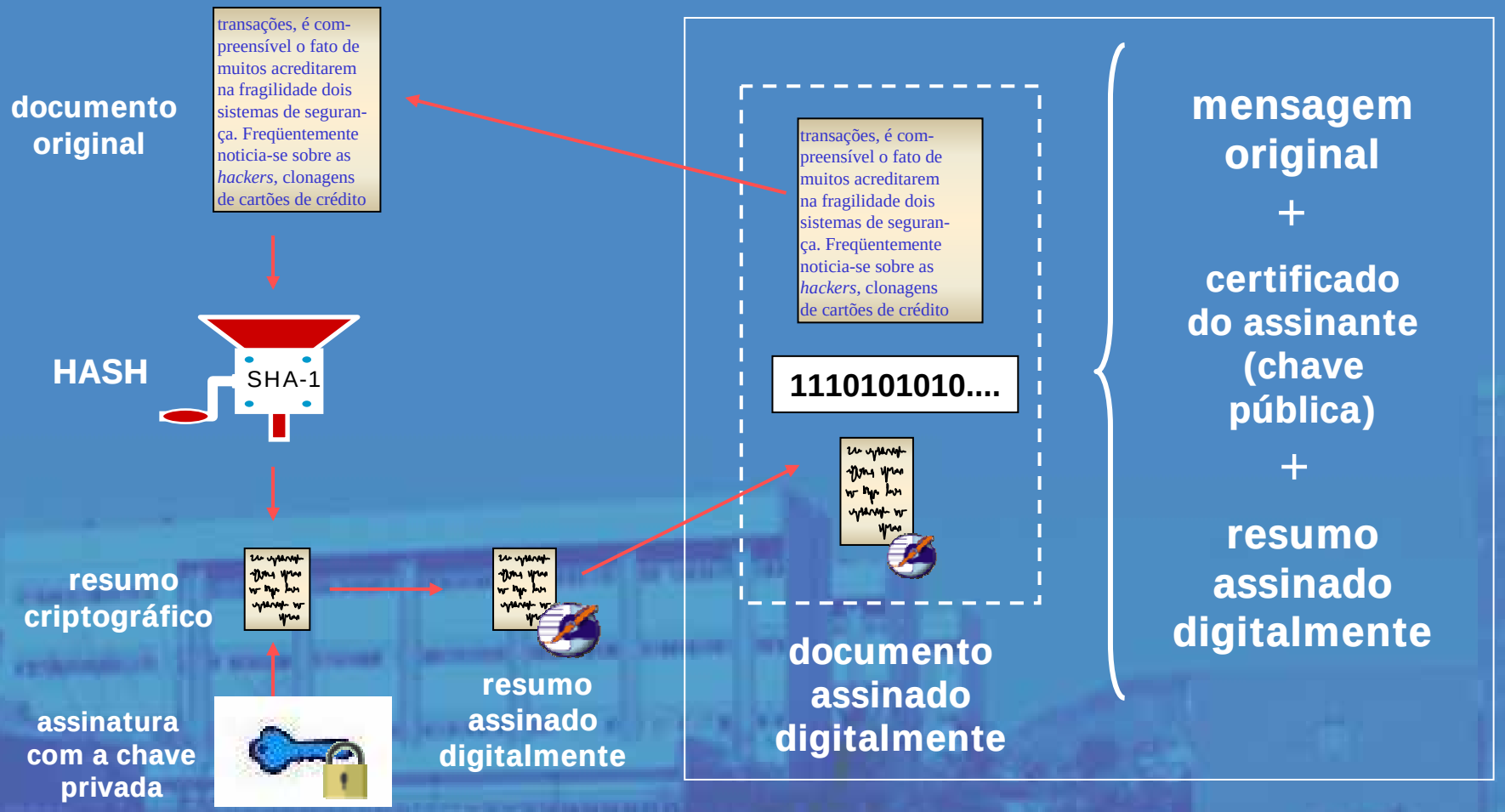
Internet: SSL provê
um encapsulamento seguro,
único e privado a dois participantes

SSL/TLS
Secure Socket Layer

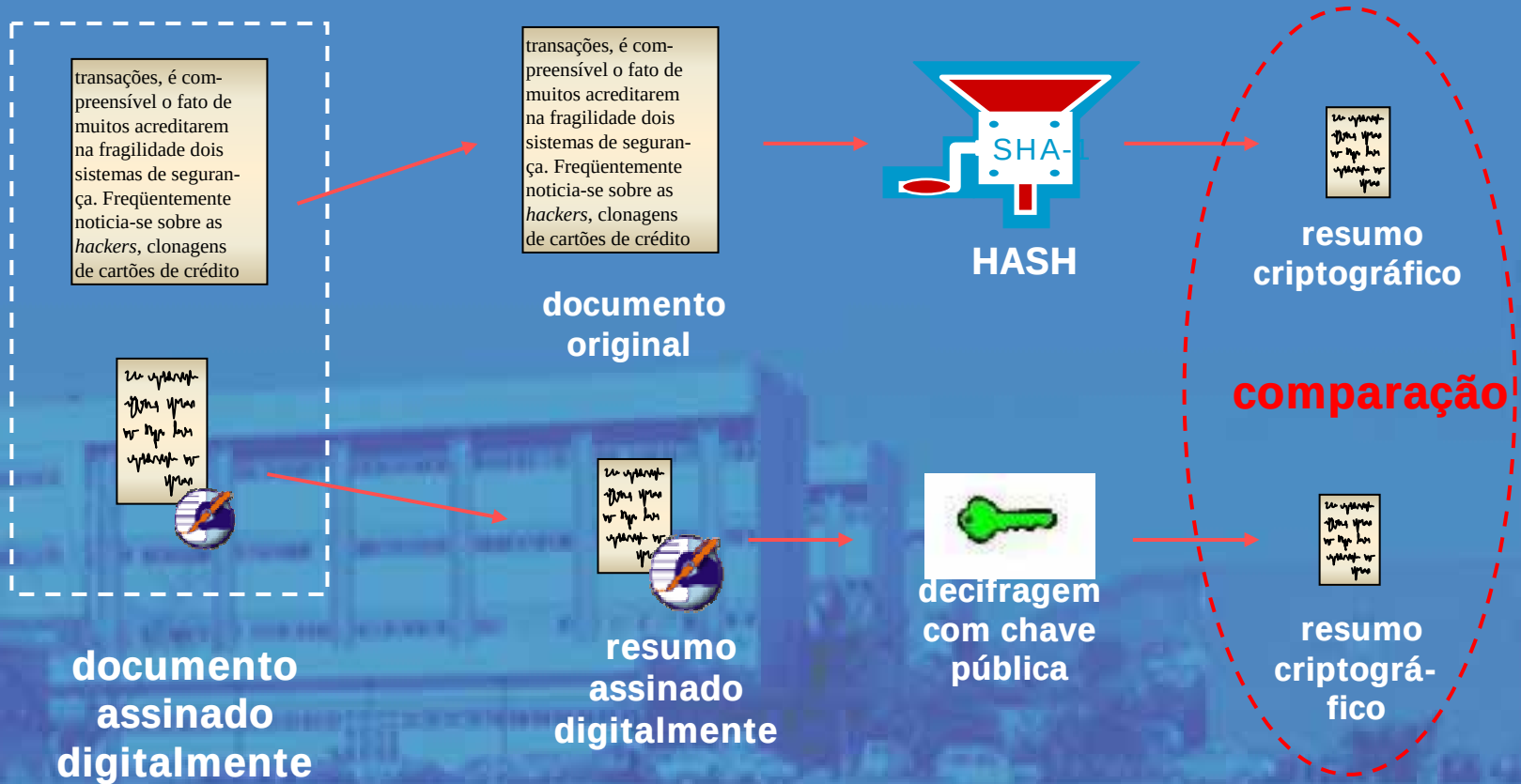
- SSL envolve 3 fases:
  1 Negociação dos algoritmos de encriptação
  2 Troca de chaves públicas e verificação de certificação, geração, encriptação e envio da chave simétrica
  3 Encriptação do tráfego de dados com chave simétrica
- Cliente e servidor negociam algoritmos:
  - cryptografia de chave pública: RSA, Diffie-Hellman, DSA ou Fortezza;
  - cifra simétrica: RC2, RC4, IDEA, DES, Triple DES ou AES;
  - funções de hash unidirecionais: MD5 ou SHA.

Autenticidade = Identidade Digital Comprovada

Composição da Assinatura digital



Autenticidade = Identidade Digital Comprovada
Verificando a Assinatura digital



www.icpbrasil.gov.br

ICP Brasil - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.icpbrasil.gov.br/

Portal CAPES AltaVista CiteSeer DBLP Webmail INF Filtros SpringerLink CNPq Brasil Telecom

Presidência da República — Destaques do governo

ICP Brasil: Infra-estrutura de Chaves Públicas Brasileira

Terça-feira, 28 de mar

- Legislação
- Comitê Gestor
- Comissão Téc. Executiva
- Fale com o ICP Brasil

ICP Brasil
O Brasil na era da certificação digital

ITI - Instituto Nacional de Tecnologia da Informação

Instalação do Certificado da AC Raiz da ICP-Brasil

Legislação
Conheça melhor a legislação da ICP-Brasil: Medida Provisória que a instituiu, criação do comitê gestor e outras normas.

O que é o ICP-Brasil

É 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.

Certificado da AC Raiz do ICP-Brasil

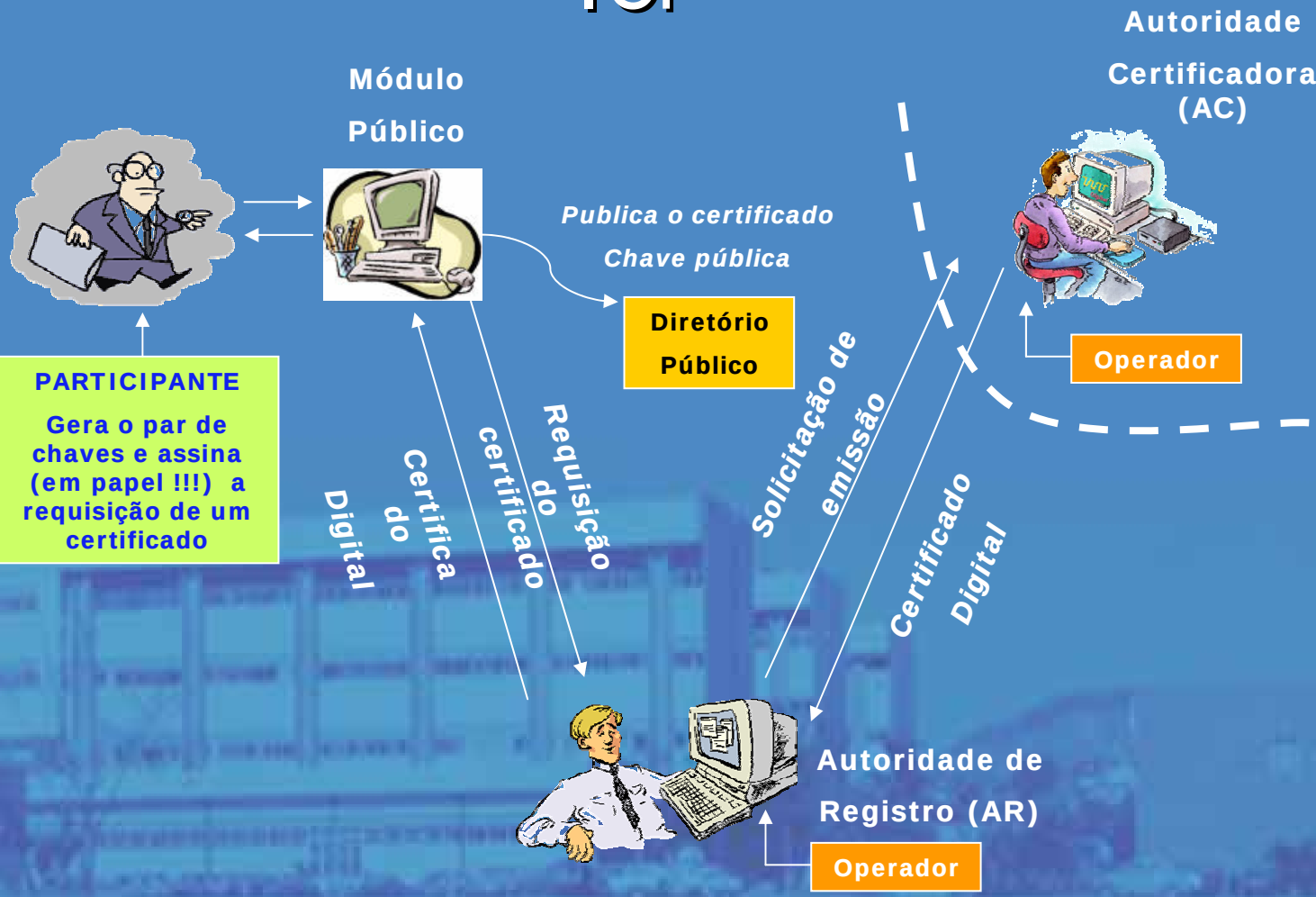
Free menu applets at www.apycom.com

The Cyclops Project
http://www.telemedicina.ufsc.br

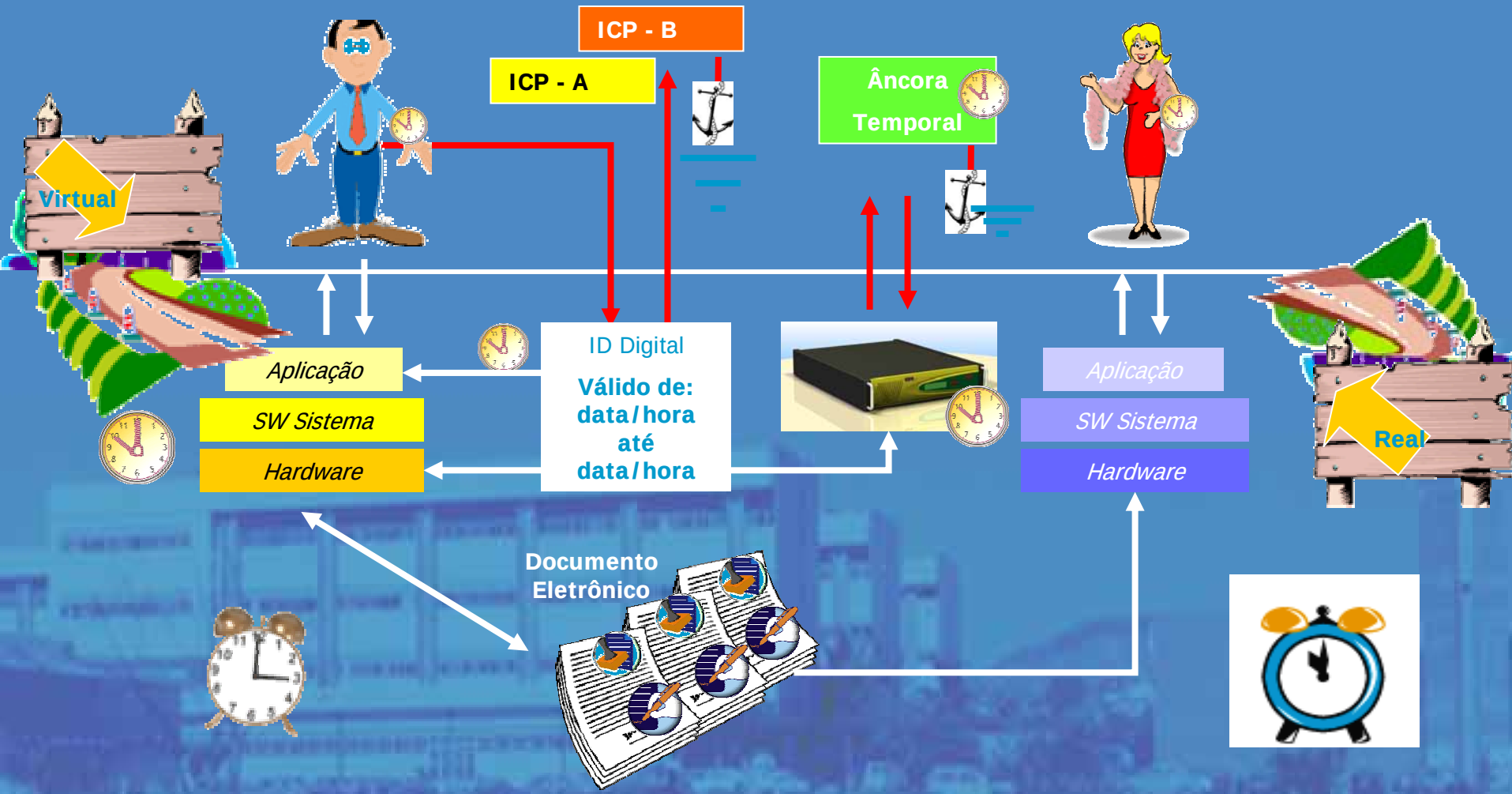
www.icp.sc.gov.br

HOSPITAL UNIVERSITÁRIO

Identidade digital
- ICP -



Âncora temporal



Sistema de tempo legal

Relógio Atômico

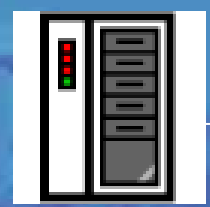
Relógio Instituto Nacional - ON

Sistema Servidor de Tempo

Aplicação de Controle

- ✓ rastreabilidade
- ✓ auditoria
- ✓ controle

Internet



Servidor de aplicação

Informação Temporal - Utilidades

- Situações de disputa
  - Comprovar que um documento foi assinado antes da revogação de um certificado digital, ou comprometimento da chave privada
  - Proposta comercial – prazo licitações
  - Patentes e propriedades intelectuais
  - Médica

Datação

- Observatório Nacional: há 10 anos - Autoridade de datação
- 1991 – Encadeamento linear
- 2001 – Protocolo entre cliente e AD
- 2002 – Método da Árvore Sincronizada

PDDE

- Composto por:
  - Plataforma computacional
  - Identidade digital
  - HSM – armazenar chave
  - Software

Datação

- Relógio do PDDE sincronizado com hora legal
- Decreto Lei 4.264 de 10 de junho de 2002 - ON – Observatório Nacional

- Absoluta/Relativa

Datação

- Absoluta: Se baseia na data e hora correntes
- Relativa: Se baseia na ordem em que os documentos são enviados à PDDE
  - Não se sabe em que momento foi protocolado
  - É possível verificar, dados 2 documentos, qual foi protocolado primeiro

Datação

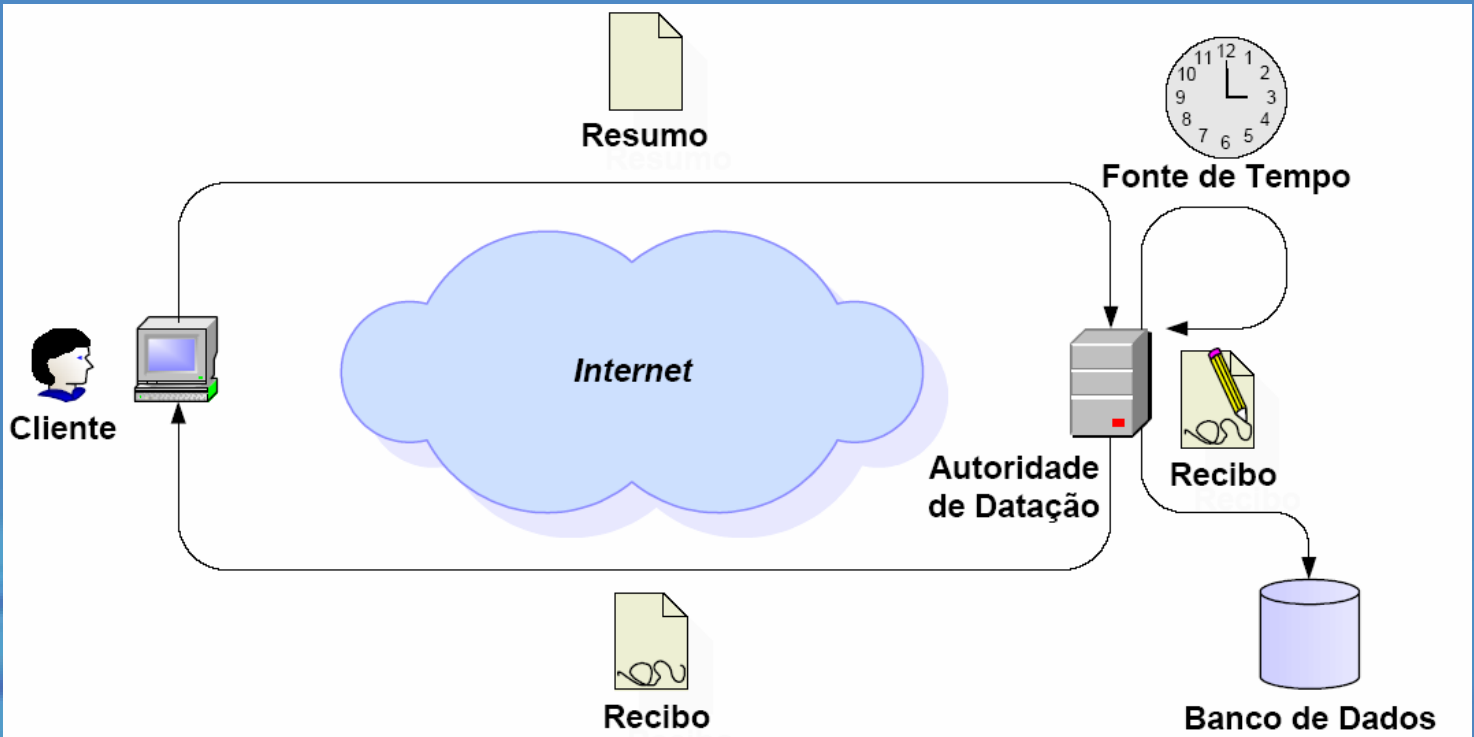


Figura 1 - Processo de Datação

Atende aos requisitos:

- **Privacidade**: Acesso ao resumo do documento, não ao documento original
- **Integridade**: Ao receber o recibo, pode-se verificar a assinatura digital da PDDE e confirmar se recibo foi alterado
- **Irrefutabilidade** – Recibo fornece evidência da existência do documento e de sua protocolação. Cliente não pode negar existência, AD não pode negar ato de protocolação

Além destes

- **Confiança** – Equipamento de datação lacrado e com padrões de segurança física e lógica; auditável
- **Facilidade de comunicação e armazenamento** – Só o resumo do documento é utilizado

Métodos de datação

- Método do Encadeamento Linear
- Método da Árvore Sincronizada

MSOffice4 Confiança na tempestividade

Item 3

; 1/5/2005

Encadeamento Linear

- Diminuir a necessidade de se confiar na AD
  - PDDE sincroniza data com AD a intervalos regulares ao invés de a toda protocolação
- Recibos são unidos formando encadeamento
  - Recibo só faz sentido no seu contexto e necessita dele
  - Função de sentido único resistente à colisão, como *Hash*

MSOffice5 Confianca na tempestividade, item 3
; 1/5/2005

Encadeamento Linear

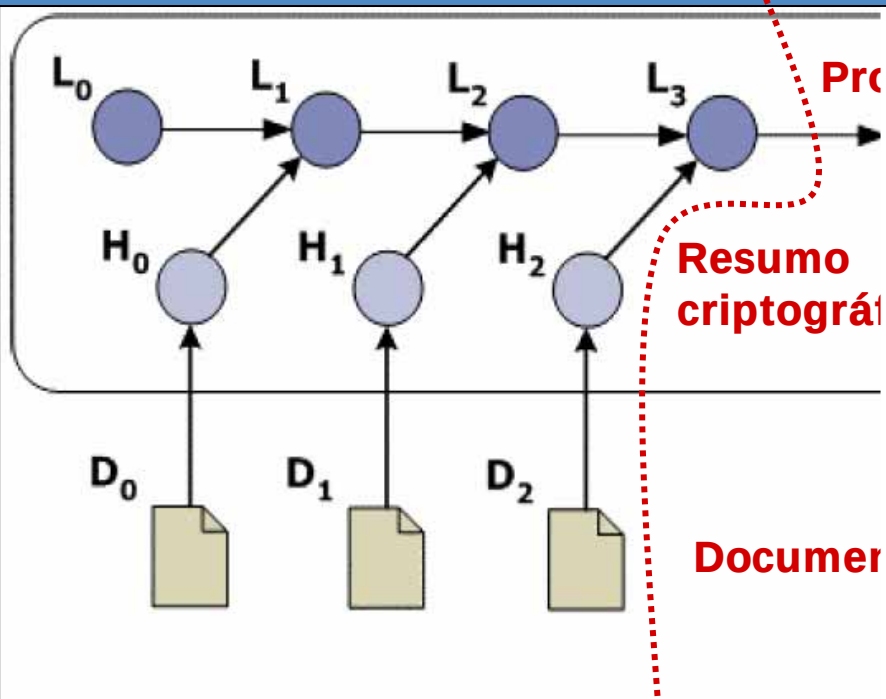


Figura 2 - Método de Encadeamento Linear

Encadeamento Linear

Forma genérica:

$$L_n = (t_{n-1}, ID_{n-1}, H_{n-1}, H(L_{n-1}))$$

t_{n-1} Data/hora documento anterior

ID_{n-1} Identificador do cliente que emitiu resumo anterior

H_{n-1} Resumo documento anterior

$H(L_{n-1})$ resumo do link anterior

Encadeamento Linear

Após cálculo do link, AD gera recibo S_n:

$$s_n = SigAD(n, t_n, ID_n, H_n, L_n)$$

SigAD(ρ) – Assinatura digital do Equipamento de Protocolação para o Protocolo ρ

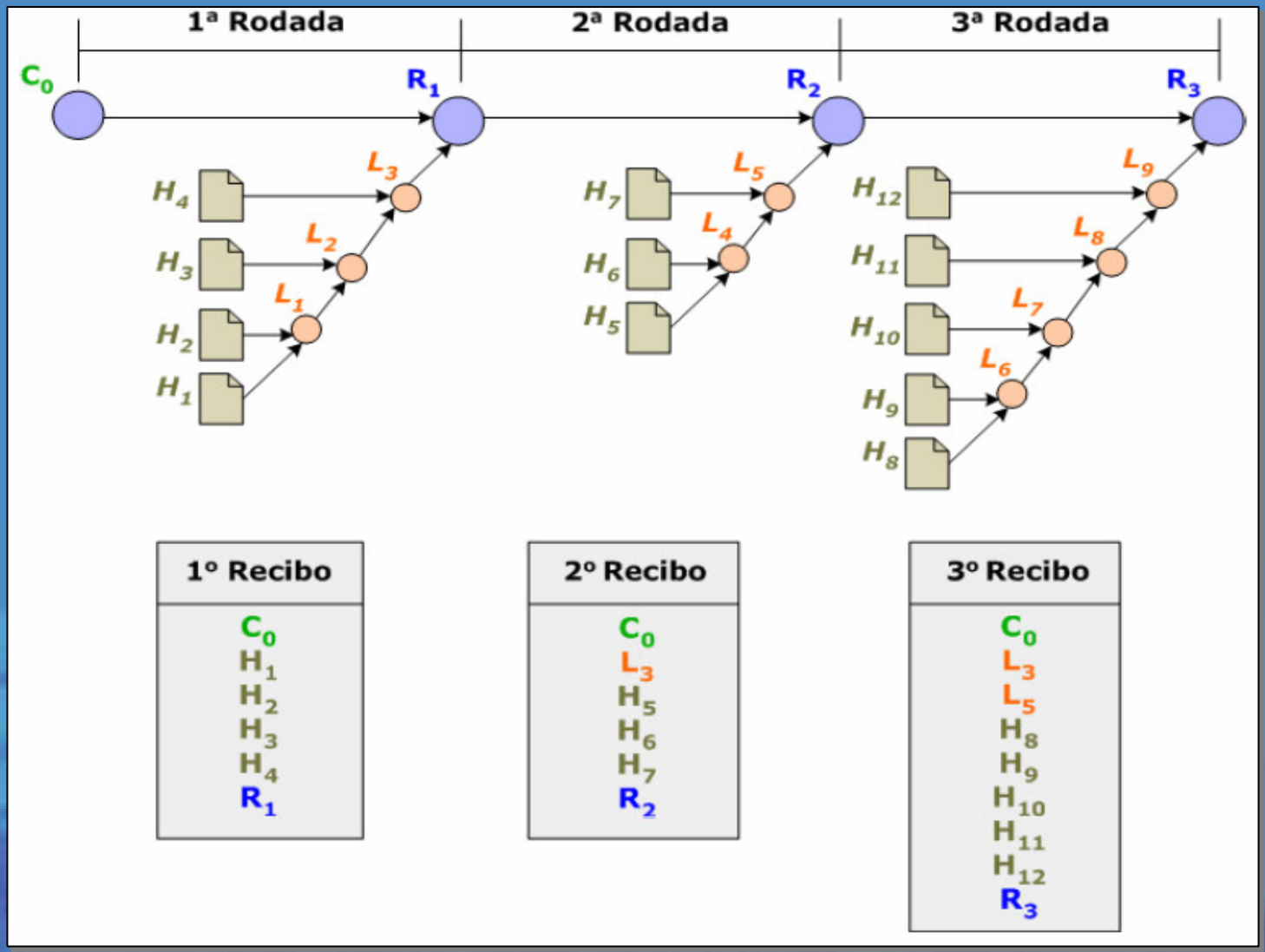
Encadeamento Linear

- Resumos dos documentos enviados a clientes ficam ordenados obedecendo a ordem de chegada
- Problemas:
  - Tempo necessário para verificar relacionamento entre dois documentos – diretamente proporcional ao número de resumos
  - Necessário armazenar toda a cadeia

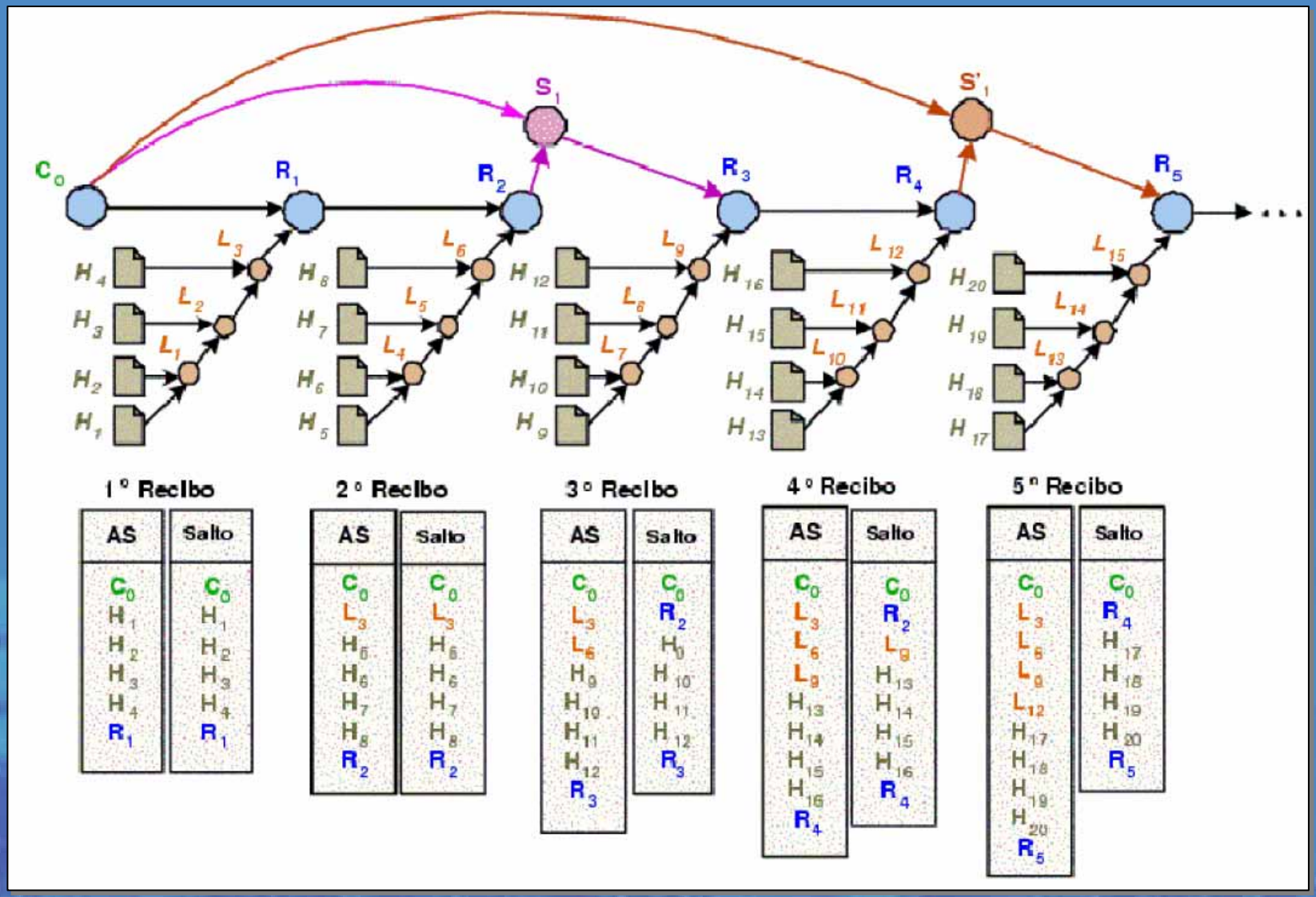
Árvore Sincronizada

- Datação relativa, com encadeamento
- Conceito de saltos para reduzir tempo de comparação da procedência entre dois documentos

Árvore Sincronizada



Árvore Sincronizada



Auditoria da protocolação

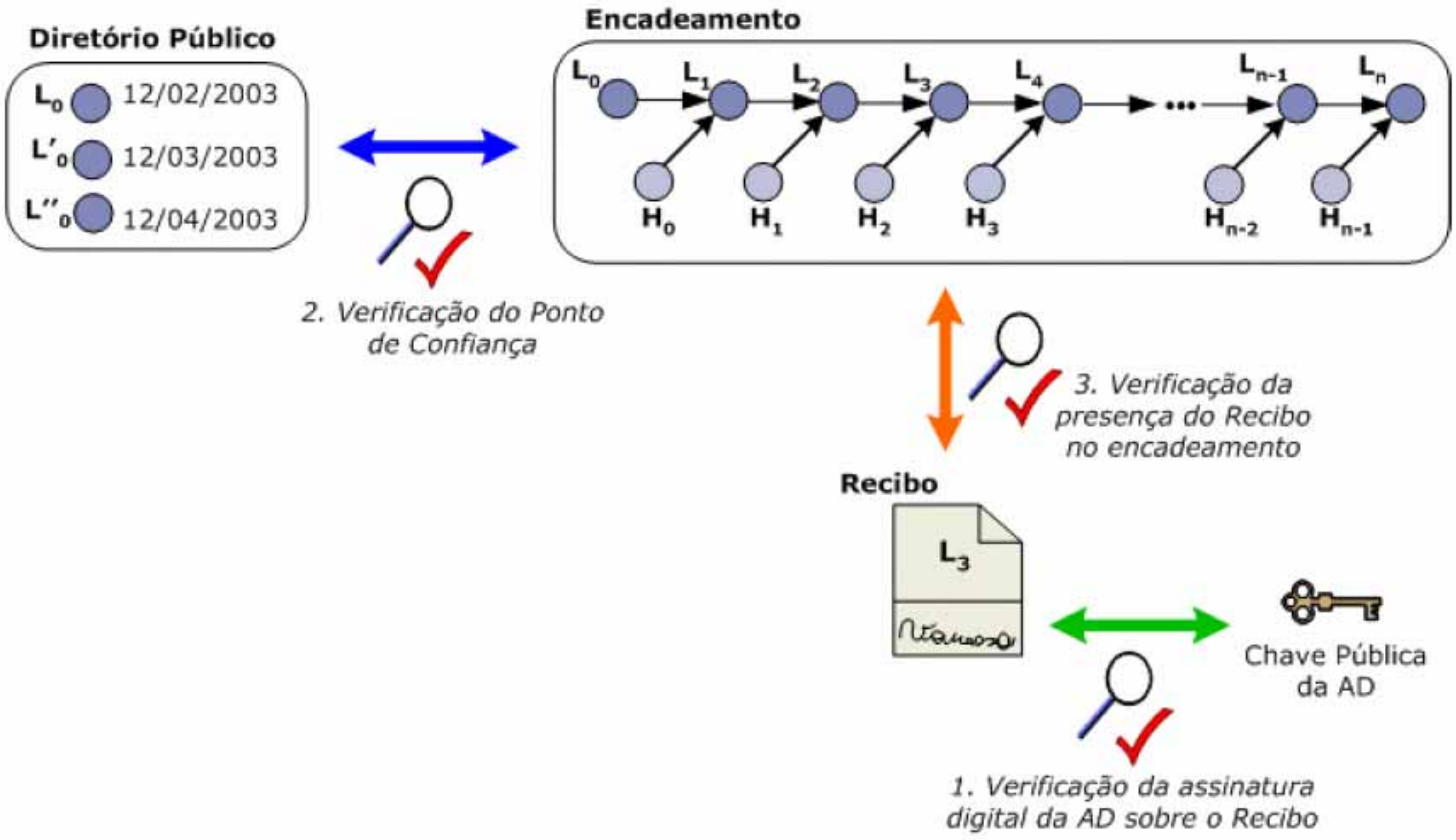


Fig. 5 – Verificação do recibo no Método do Encadeamento Linear

MSOffice6 Confianca item 4
; 2/5/2005

Auditoria da protocolação

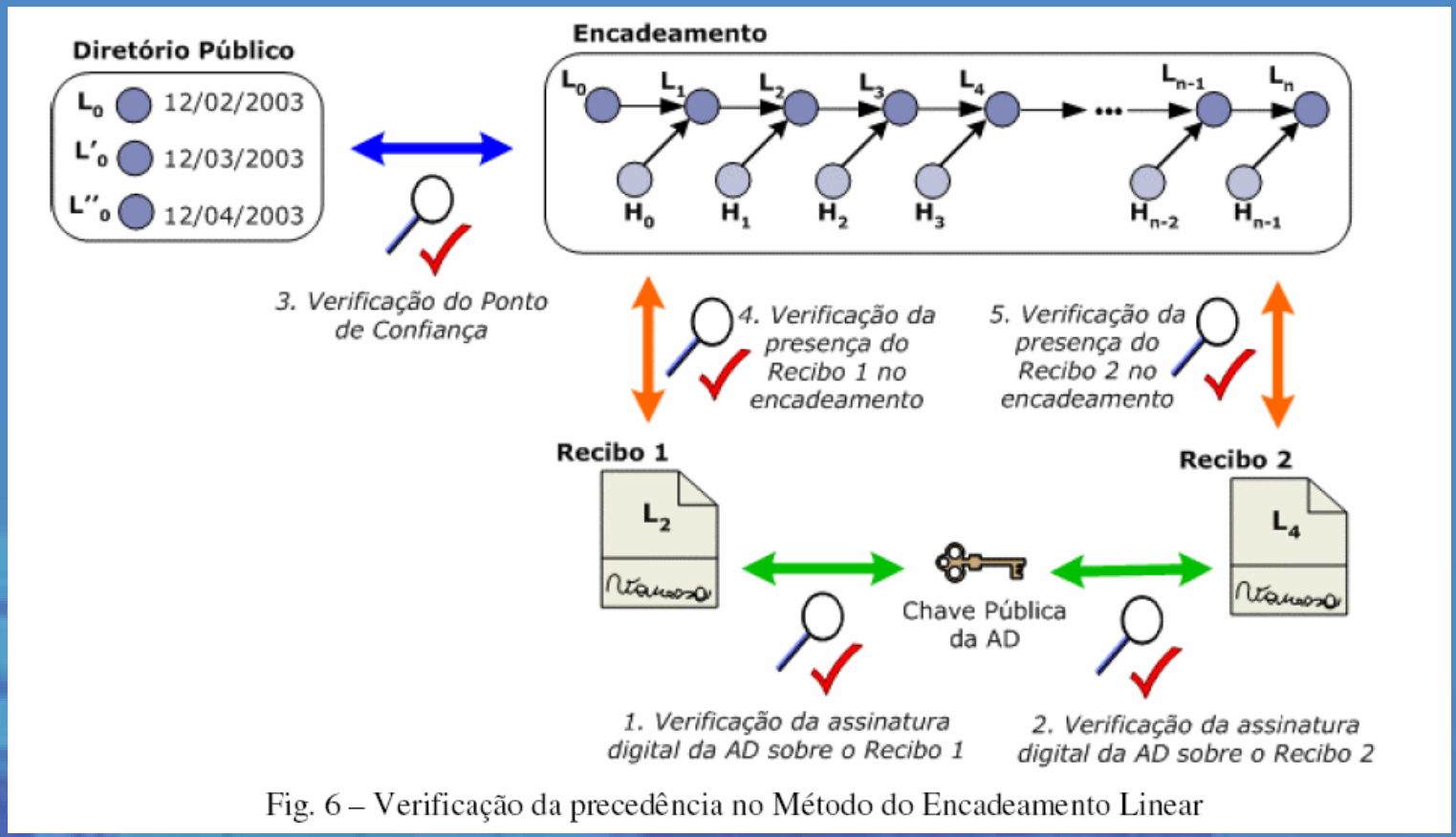


Fig. 6 – Verificação da precedência no Método do Encadeamento Linear

Auditoria

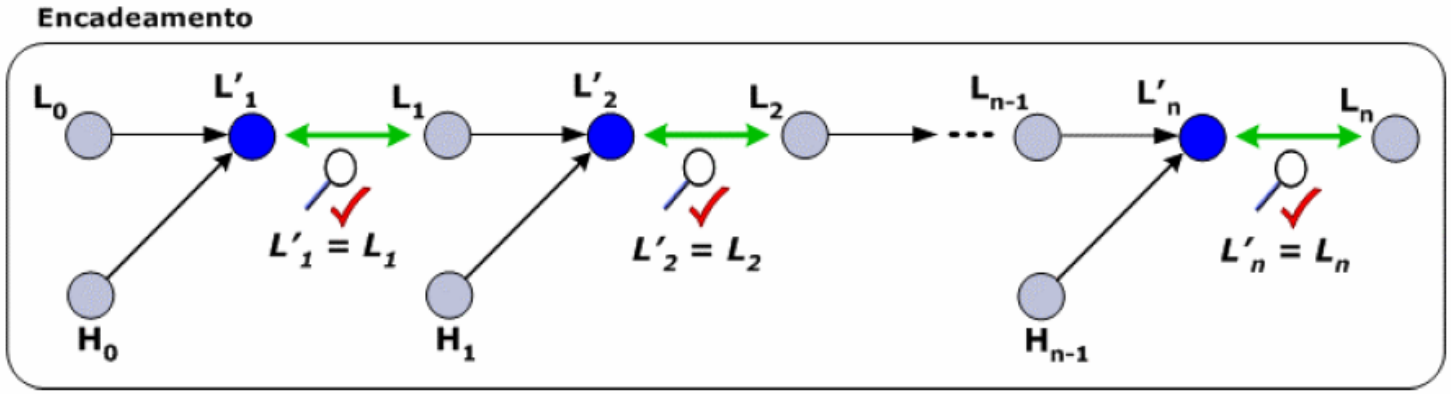


Fig. 7 – Verificação da integridade do banco de dados no Método do Encadeamento Linear

Auditoria

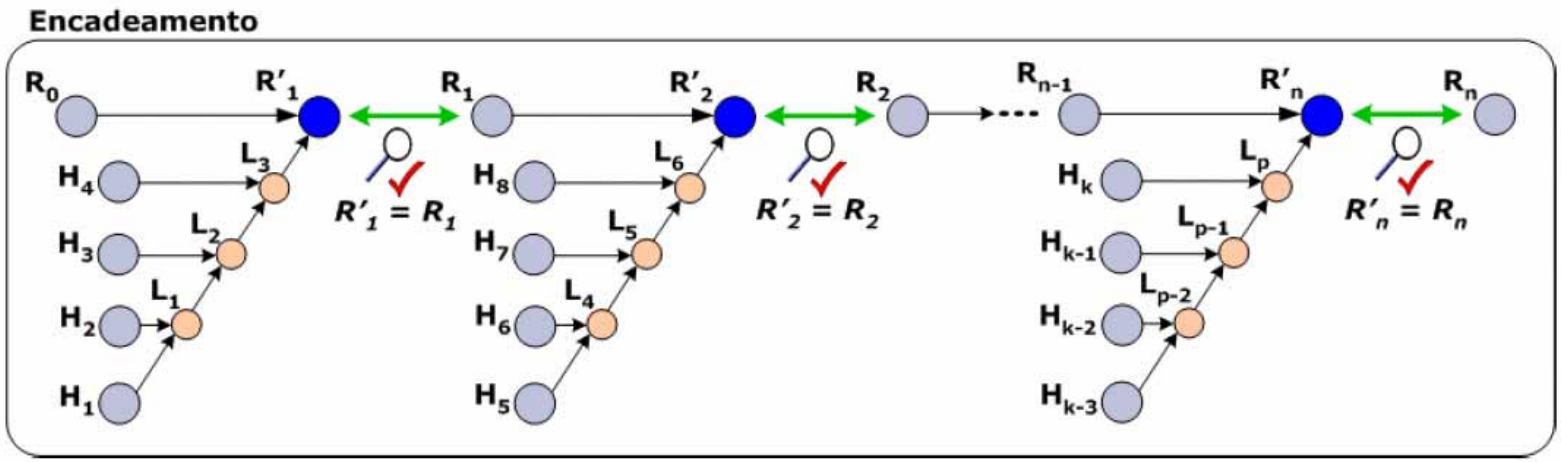


Fig. 8 – Verificação da integridade do banco de dados no Método da Árvore Sincronizada

2. Mercado

- Bry
  - www.bry.com.br


BRy Tecnologia - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://www.bry.com.br/servicos/pdde/testdrive.asp
tecnologia
Empresa Produtos Serviços Suporte Alianças Downloads Comprar
Protocolação Digital
Sobre o serviço
Test-Drive
Adquirindo o Serviço
Loja BRy
Contato
Notícias
Mapa do site
Acessar sua conta
:: Test-Drive
A BRy oferece a você a possibilidade de fazer um test-drive no sistema de protocolação digital de forma totalmente gratuita. Essa é uma oportunidade única para você conhecer melhor o serviço e comprovar a facilidade do seu uso.
Antes de acessar o sistema, sugerimos a compreensão do processo de protocolação. Leia mais aqui.
Selecione a operação desejada:
Protocolar Documento
Verificar Protocolação
Recuperar Documento
Done

NCipher

- pdfProof
  - Assina e emite recibo de tempo
  - Utiliza um único certificado digital
  - Hardware protege as chaves
- DSE 200
  - Hardware de rede e toolkit para desenvolvedores com interfaces para interação com softwares diversos
- TimeSource Master Clock
  - Relógio atômico de rubídio, NTP

http://www.ncipher.com

nCipher Digital Signature & Time Stamping Solutions - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.ncipher.com/timestamping/

DTS

Google Search: timesta... | nCipher | Partners | Safe... | nCipher Digital Signa... | RSA Security - 7.11 Wh... | FORTEZZA™ CRYPT...

COMPANY PRODUCTS SOLUTIONS RESOURCES PARTNERS SUPPORT INVESTORS SEARCH

nCIPHER

- Product Overview
- Hardware Security Modules
- SSL Accelerators
- Time Stamping & Document Sealing
- Database Encryption
- Developer Toolkits
- Core Technologies
- How to Buy

Digital Signature & Time Stamping Solutions

If you don't sign your electronic documents...

- Anyone in an organization can potentially falsify documents
- Time, identity and integrity cannot be proven
- The validity of documents and transactions can be challenged and court cases will be lost
- Executives put themselves in danger of civil and criminal prosecution

In the paper world documents can be notarized, post marked and signed by witnesses to attest to authenticity. In the electronic world, robust safeguards are essential if electronic documents are to be used as evidence for future dispute resolution; as a result digital signatures have emerged as the standard for document security.

A digital signature accomplishes three important things:

- **Who:** It identifies who signed the document by binding the identity contained in a digital certificate to the document
- **What:** It creates a cryptographic 'hash' which mathematically identifies the content of the

Find: Find Next Find Previous Highlight

Transferring data from www.ncipher.com...

Mykotronx

- Cryptocard
  - Cartão PCMCIA
  - Encripta/Decripta
  - Assina
  - Troca de chaves/Hash
  - TimeStamping
  - National Security Agency-certified CAPSTONE RISC-based cryptographic processor
  - Self-contained, tamper-resistant, real-time clock

FORTEZZA™ CRYPTOCARD - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.mykotronx.com/products/fortezza/crypto.asp

DTS

Google Search: timestamping hardware ... | RSA Security - 7.21 What is tamper-resi... | FORTEZZA™ CRYPTOCARD

MYKOTRONX INC A SAFENET, INC. COMPANY

SOLUTIONS | PRODUCTS | ABOUT MYKOTRONX | NEWS & EVENTS | INVESTOR INTEREST | CONTACT US

FORTEZZA®

The Next Generation Solution for INFOSEC Applications

Mykotronx Home : Products : Fortezza : FORTEZZA™ CRYPTOCARD

FORTEZZA™ CRYPTOCARD

FORTEZZA™ CRYPTOCARD

Type 2 Encryption/Decryption, Secure Hash, and Key Exchange
The Mykotronx FORTEZZA™ Cryptocard implements cutting-edge cryptographic security and authentication methods in a PCMCIA hardware token for Government and commercial applications.

Self-contained, standardized, and easily integrated, the Card provides the ultimate in portable security, together with on-board storage of user credentials, keys, and digital certificates.

Fully FORTEZZA™ compliant, the card incorporates the National Security Agency-certified CAPSTONE RISC-based cryptographic processor. It is the hardware crypto token chosen to secure the Defense Messaging System (DMS).

More about FORTEZZA™ Cryptocard

» Benefits

RELATED LINKS

- FORTEZZA Data Sheet (PDF)
- Mykotronx Products Overview
- Mykotronx Solutions
- Homeland Security Solutions
- Mykotronx Home Page
- SafeNet, Inc.

Find: timesta | Find Next | Find Previous | Highlight

Done

About Authentic Document IDs

What is digital notarization?

Digital notarization is a timestamping service that lets you prove the existence and state of an electronic document at a fixed point in time by creating a digital receipt.

What is a digital fingerprint or hash file?

Often described as a digital fingerprint, a hash is simply a "summary" generated from a digital document using a mathematical rule or algorithm. It is designed so that a small change in the document would produce a big change in the hash. Hashing algorithms are "one-way": you can create a hash from a document, but you cannot recreate the document from a hash. A hash is not an encryption of the document. Most importantly, it's very difficult to find two documents that have the same hash.

The Authentic Document Service uses hash files because a small (but important) change in a document (like changing US$100,000 to US$1,000,000) would produce a completely different hash.

What is an Authentic Document ID?

An Authentic Document ID is a Class 3 certificate that allows you to perform digital notarizations, using VeriSign's Authentic Document Service, for the purpose of authenticating documents. VeriSign Authentic Document IDs are used to create and send a signed fingerprint (hash) of the original document to VeriSign's Authentic Document Service (the original document never leaves the requestor's personal computer). Upon receipt, the Authentic Document Service verifies the validity of the signature. After the signature is verified, the signed fingerprint is digitally time-stamped to create a digital receipt, which is delivered to the requestor's personal computer. The signed fingerprint submitted by the requestor is also stored by VeriSign, and can be made accessible to the appropriate parties at a later date for dispute resolution and auditing purposes.

- **Developer Solutions**
- VeriSign Software Development Kits (SDKs) allow software service and application developers and service providers to create custom applications enabled for specific Public Key Infrastructure (PKI) functionality, including digital notarization and document authenticity verification. To learn more about VeriSign SDKs, contact an Internet Sales Representative at (650) 426-5112 or (866) 893-6565 or contact sales.
- **Digital Notarization SDK:** Includes a programmatic interface to digitally notarize and verify content authenticity from within your application. *VeriSign authenticates the document by acting as a "third party witness"* to the document's state at a particular time. Enables audit trails and digital receipts.
- **Certificate Validation SDK:** Gives software real-time certificate status for any of the 3+million certificates issued by VeriSign. Leverages industry and Internet PKI standards including OCSP and X.500 Certificate Revocation Lists. This is available for a multitude of platforms including Windows.
- **Smart Cards:** Scalable, flexible, and customizable solutions for incorporating certificates into smart cards an efficient, flexible, and portable solution for authenticating identities, encrypting data, and validating transactions

Slide 59

MSOffice8 http://www.verisign.com/products-services/security-services/code-signing/brew-document-ids/faq.html#01000003
; 4/5/2005

- Adaptador PCI
- Auditável, compatível com Microsoft Crypto API e JAVA JCA/JCE
- Several tamper detection mechanisms
- On board Real Time Clock
- Hardware based true random number generator with ANSI X9.31 whitener
- Smart card based authentication and secure key export/ import

- **TimeCertain's Chronologics® TimeServer** – Aliança da TimeCertain com a eracom - Servidor para Linux que utiliza o hardware e o relógio deste para fazer TimeStamps

http://www.eracom-tech.com/products/pso/pso.htm

eracom TECHNOLOGIES

protect the future

Transaction Security

Hardware Security Modules

- ProtectHost Orange
- ProtectHost White
- ProtectServer Orange External
- ProtectServer Orange
- ProtectServer Blue

Cryptographic APIs

- ProtectToolkit C
- ProtectToolkit J
- ProtectToolkit M
- ProtectToolkit ESA
- ProtectToolkit RSA
- ProtectProcessing
- Mark II

Privacy of Information

- ProtectFile Business
- ProtectFile Premium
- ProtectDrive
- ProtectPack

Hardware Security Module - HSM

ProtectServer Orange™

Public Key Infrastructures (PKI) enable trust between people and organizations trading electronically.

Eracom's hardware security module, ProtectServer Orange intelligent FIPS 140-1 Level 3 certified cryptographic PCI adapter is designed to enable that trust.

Comprising a new generation PCI Bus adapter and open standard software APIs, ProtectServer Orange™ is intended for use where physical and logical protection against malicious access to cryptographic keys is required.

Designed for Microsoft® Windows® Server 2003

ProtectServer Orange is an Eracom Hardware Security Module (HSM) that combines security and speed in an all-in-one product with key storage and cryptographic operations performed within the device's certified FIPS 140-1 level 3 perimeter. Protectserver Orange is supported by most popular server platforms, while other unsupported platforms can utilize remote client/server products.

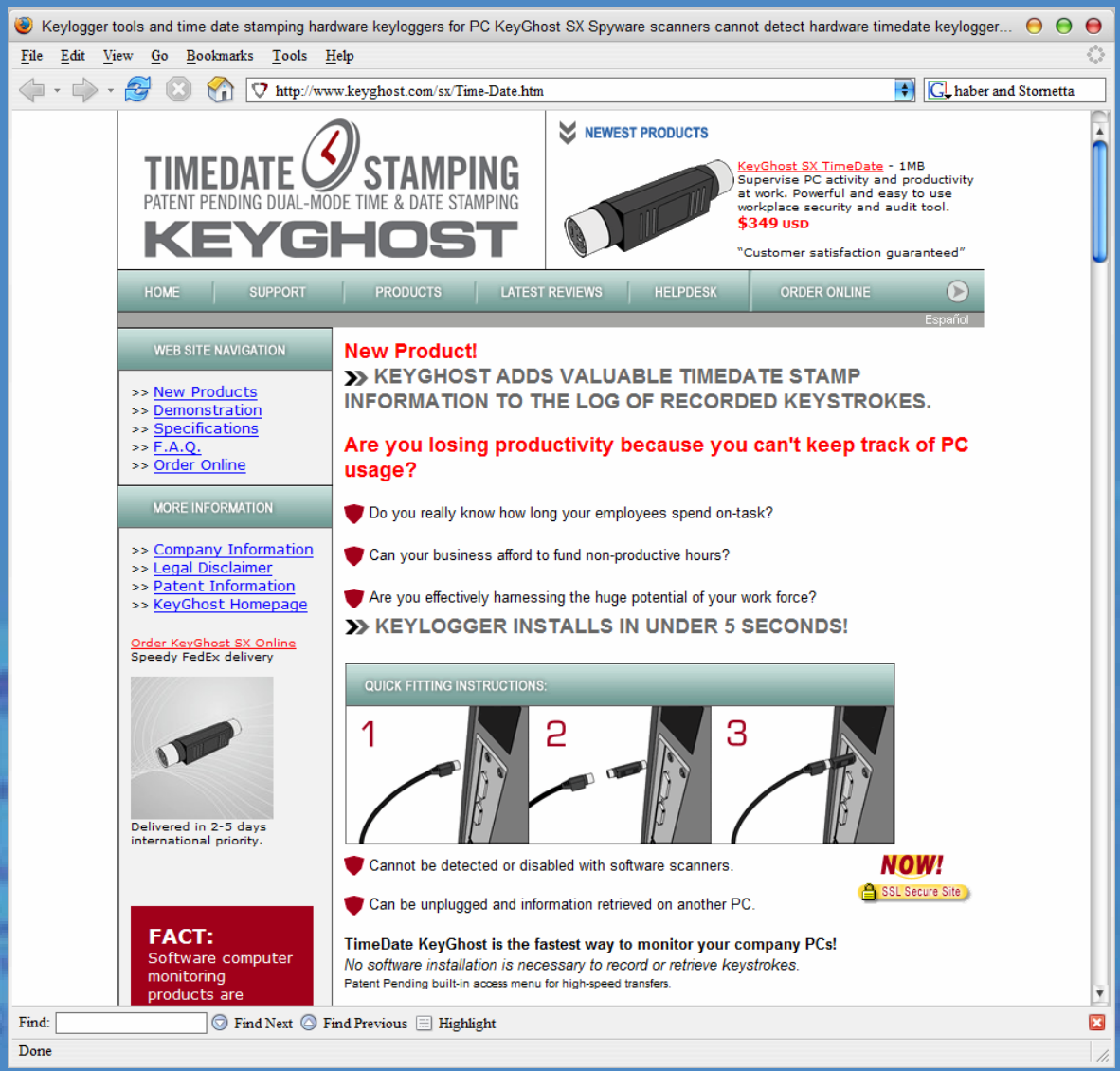
Existing applications relying on PKCS#11, Java JCA/JCE and Microsoft Crypto API interfaces can utilize ProtectServer Orange hardware based security and performance transparently. All accesses to the device are subject to control and audit with only authorized users or applications permitted access to Protectserver Orange controlled resources and facilities. All accesses - successful or not - can be recorded in an audit log.

Designed for Microsoft® Windows® XP

Several tamper detection mechanisms are provided and activation of one or more of these will erase the secure memory. With 1Mb of key storage, Protectserver Orange is suited for applications where a large amount of keying and

Curiosidade: KeyGhost

- Keylogger para interface de teclado PS/2
- Guarda seqüência de teclas e momento no tempo de cada apertar de tecla



3. Legislação
SBIS - Sociedade Brasileira de Informática em Saúde

- Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (RES)

SBIS

- CFM recebe uma série de solicitação de pareceres a respeito da legalidade da utilização de sistemas informatizados para capturar, armazenar, manusear e transmitir dados do atendimento em saúde
- Substituição do papel pelo formato eletrônico

SBIS

- CFM
- Sociedade Brasileira de Informática em Saúde
- ASSESPRO
- Ministério da Saúde
- AMB
- CONASS
- CONASEMS
- ANVISA
- ANS
- FBH
- CONARQ
- ABRAHUE

SBIS

- Complexidade do tema
- Separar certificação do
  - Produto de software
  - Processo de uso

SBIS

- Certificação em três etapas
  - Produto de software – Etapas 1 e 2, com SBIS e CFM
  - Processo de uso do sistema informatizado – Todas as instituições

SBIS

- Requisitos de segurança, conteúdo e funcionalidades que um RES deve atender para estar em conformidade com as
- Resoluções do CFM Nos. 1638 e 1639

CFM - Res.1638

- O que é prontuário médico
- Quem é responsável pelo prontuário
- Itens que devem constar obrigatoriamente

MSOffice7 Item 2.1 Pagina 11 SBIS
; 3/5/2005

CFM - Res.1639

- Aprova as “Normas Técnicas para o Uso de Sistemas Informatizados para a Guarda e o Manuseio do Prontuário Médico”, possibilitando a elaboração e o arquivamento do prontuário em meio eletrônico

SBIS

- Prazos
  - Mínimo de 20 anos, a partir do último registro, para preservação dos prontuário em suporte papel
  - Autoriza, em caso de microfilmagem, eliminação do suporte de papel (Lei n. 5.433/68 e Decreto n. 1.799/96) (após análise pela comissão)
  - Autoriza, em caso de digitalização, a eliminação do suporte em papel, desde que obedeça à norma específica de digitalização

SBIS

- Comitê ISO 215: Registro Eletrônico em Saúde

Padronização na área de informação em saúde e tecnologia da informação com o objetivo de atingir a compatibilidade e a interoperabilidade entre sistemas independentes. Garantir a compatibilidade de dados para fins de análise estatística, reduzindo redundâncias e a duplicação de esforços.

SBIS

- 23 países membros
- 14 países na categoria “O”

- Só países membros têm direito a voto

- Brasil é... Bom, um caso à parte

SBIS

- Organizado em grupos de trabalho:
  - I: Registro de Saúde e Modelagem
  - II: Mensagens e Comunicação
  - III: Representação de conceitos em Saúde
  - IV: Segurança

ISO TC 215 Working Group 4
Health Informatics - Security

Scope

Meeting Dates

Documents

Current Work Items

Contact Details

Current Work Items

1. Discussion on the received comments on the CD on Data protection (Ray Rogers).
2. Discussion on "Security requirements for archiving and backup - Archiving of health records (TS)" (Pekka Ruotsalainen)
3. Discussion on "Directory services for communications and identification of professional and patient (TS)" (Lori Reed Forquet)
4. Discussion on preliminary work items.
   "Framework for health information security" (Ted Cooper)
   "Privilege management and access control" (Bernd Blobel)
5. Other issues
   "Security requirements for archiving and backup - Guidelines for backup" (Ernst Leitgeb)

Related Links

Public Key Certification Infrastructure

Australia
The Australian Government's public key authentication framework project from Project Gatekeeper :
(http:// www.gpka.gov.au/information-sheets/execsum/execsum.htm)

A more complete description of the initiative
(http://www.gpka.gov.au)

"Strategies for the Implementation of a Public Key Authentication Framework (PKAF) in Australia - SAA MP75-1996"
(http://www.acs.org.au/ president/1996/epubs/pkaf.htm)

SBIS

- Documentos do grupo 1 – Base para certificação de software da SBIS
  - ISSO/PRF TS 18308 – Health Informatics – Requirements for na electronic health record architecture (Final Draft)
  - ISO/TC 215 Technical Report – Electronic Health Record Definition, Scope and Context. Second Draft

SBIS

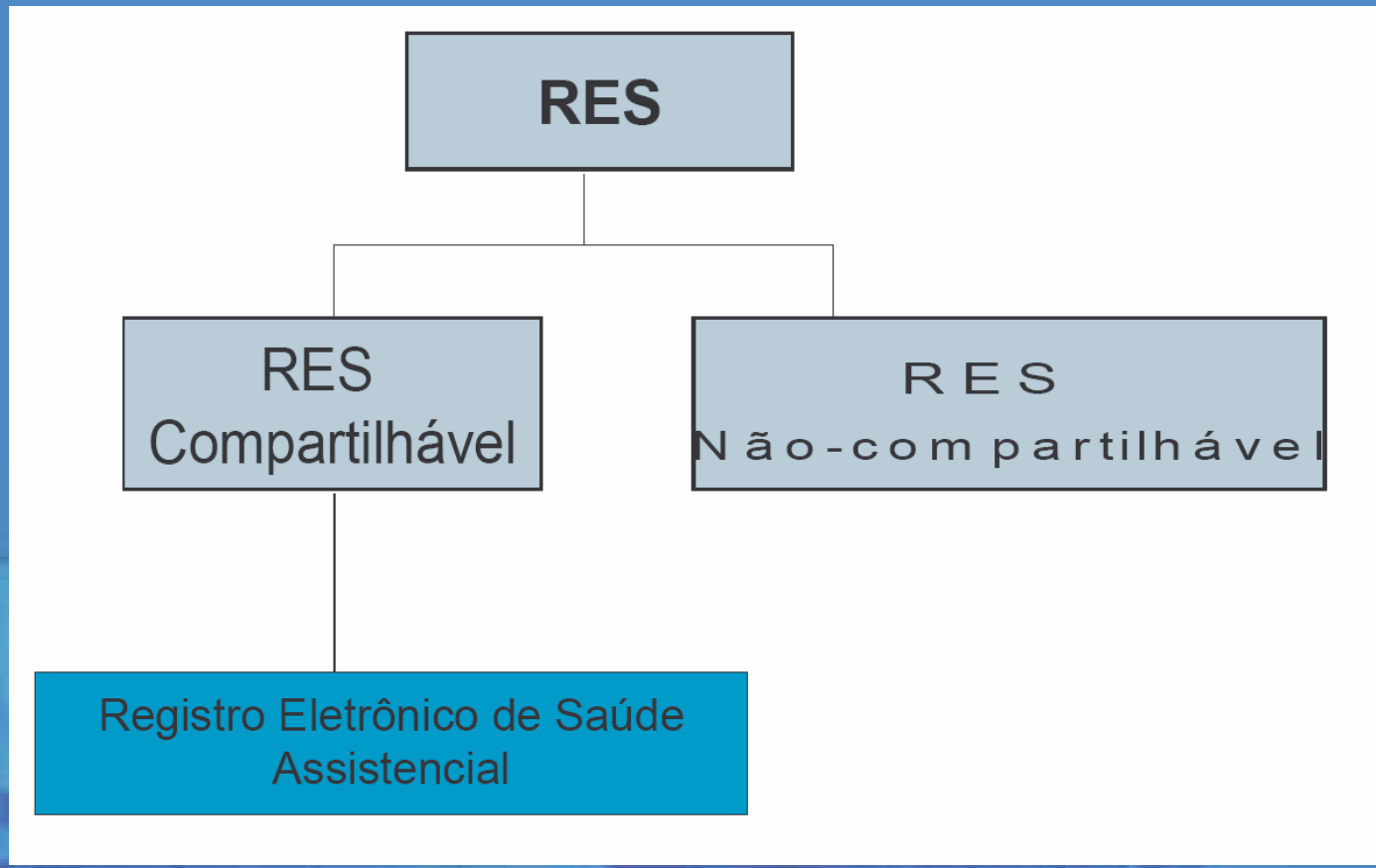
- RES

Institute of Medicine: "Prontuário Eletrônico do Paciente é um registro eletrônico de dados do paciente armazenado num sistema capaz oferecer aos usuários a disponibilização de dados confiáveis e recursos como lembretes e alertas, sistemas de apoio à decisão, links para bases de conhecimento médico e outros."

Computer-based Patient Record Institute: "Um registro computadorizado de paciente é uma informação mantida eletronicamente sobre o status e cuidados de saúde de um indivíduo durante toda a sua vida."

Murphy, Hanken e Waters, 1999: "Um registro eletrônico de saúde é qualquer informação relacionada com o passado, presente ou futuro da saúde física e mental, ou condição de um indivíduo, que reside num sistema eletrônico usado para capturar, transmitir, receber, armazenar, disponibilizar, ligar e manipular dados multimídia com o propósito primário de um serviço de saúde."

SBIS


RES
RES Compartilhável
RES Não-compartilhável
Registro Eletrônico de Saúde Assistencial

SBIS

- Definições
  - **RES** - *Repositório de informação a respeito da saúde de um ou mais indivíduos numa forma processável eletronicamente*
  - **RES Compartilhável** – *um RES com um modelo padronizado de informação, independente do sistema de RES e passível de acesso por vários usuários autorizados utilizando diferentes aplicações.*
    - *Idéia é apoiar o processo assistencial*

SBIS

- **RES Assistencial**

um repositório de informação a respeito da saúde de um ou mais indivíduos em forma processável por computador, armazenada e transmitida de forma segura e passível de acesso por vários usuários autorizados em diferentes aplicações. O RES-A possui um modelo padronizado de informação, independente do sistema de RES. O objetivo principal do RES-A é apoiar a continuidade, eficiência e qualidade da assistência integrada. O seu conteúdo de informação é retrospectivo, atual e prospectivo.

Idéia é que existam vários RES-A, com conjuntos de dados específicos para cada contexto em saúde. Por exemplo:

- RES-A para acompanhamento da assistência pré-natal
- Doenças crônicas

SBIS

- Normas para requisitos de segurança, baseadas
  - NBR ISO 17799
  - ISO 15408

SBIS

- ICP-Brasil – Infra estrutura de chaves públicas brasileira

- MP N. 2.200-2, 24 agosto 2001, regulamentação da assinatura digital no Brasil

SBIS

- Alguns trechos:

Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1o As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiras em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1o de janeiro de 1916 - Código Civil.

§ 2o O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

SBIS

- Escopo da certificação
  - Categoria Assistencial
  - Categoria SADT
  - Categoria Gestão
- "*Propositalmente as definições são amplas e abrangentes, para que qualquer sistema que capture, armazene, apresente, transmita ou imprima informação identificada em saúde poderá se submeter ao processo de certificação*"

SBIS

- Processo é voluntário
- Dividido em fases
  - Fase I: Declaração de conformidade
  - Fase II: Selo SBIS/CFM
  - Fase III: Certificação de RES
- No momento, I e II – Produto
- III: Ministério da Saúde e ANVISA

SBIS

- Fase I – Declaração de conformidade
  - Segurança, conteúdo e funcionalidades em conformidade com o documento
  - “Modelo de Declaração de Conformidade”

SBIS

- Fase II – Selo SBIS/CFM
  - Produto de software será auditado
  - Voluntária
  - Dois auditores, etc.

SBIS

- Fase III – Certificação de PEP
  - Modelo mais amplo, permite que façam pleno uso do RES e possam abandonar o prontuário em papel com segurança
  - Idéia é adotar metodologia no estilo da ONA, envolvendo todas as entidades
  - Legislação a ser legitimada, discutida com Miniestério da Saúde, etc. Previsão para o fim de 2005

SBIS

- Níveis
  - NGS1 – Sistemas de registro eletrônico com assinatura manual (SRESAM)
  - NGS2 – Sistemas de registro eletrônico com assinatura digital (SRESAD)

  - NGS1 jamais autorizados a abandonarem papel, conforme resolução CFM e legislação
  - Em princípio autorizados a substituírem o papel

SBIS

- Critérios de avaliação que garantem nível de segurança.
- A total aderência é indispensável e imprescindível para conclusão do processo de certificação

SBIS

SBIS

FDA

- FDA 21 CFR Part 11
- A – Provisões gerais
  - Escopo
  - Implementação
  - Definições
- B – Documentos/registros eletrônicos
  - Controle para sistemas fechados
  - Controle para sistemas abertos
  - Manifestações de assinaturas
  - Linking de assinaturas/registros
- C – Assinaturas eletrônicas
  - Requisitos gerais
  - Componentes e controles
  - Controle para códigos de identificação e senhas

FDA

- **Escopo**
- Considera registros eletrônicos, assinaturas digitais e manuscritas sobre registros eletrônicos autêntica e equivalente a registros em papéis e assinaturas manuscritas executadas sobre papel
- Igual desde que não especificado em regulamento após 20 agosto 1997
- Todo sistema computadorizado (hardware, software, controles e documentação) deve estar disponível e sujeito a inspeção pelo FDA

FDA

- Implementação
  - Pode-se usar registros eletrônicos ao invés de registros em papel; bem como assinaturas digitais ao invés de assinaturas manuscritas em papel, desde que todos os requisitos sejam preenchidos

FDA

- Subpart B – Registros eletrônicos

- *Pessoas que utilizam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles designados a garantir a **autenticidade, integridade** e, quando apropriado, **privacidade** de registros eletrônicos, e a garantir que o signatário **não pode repudiar** o registro assinado como não genuíno.*

FDA

- Subpart B – Registros eletrônicos
- Controles para sistemas fechados
- *Pessoas que utilizam sistemas fechados para criar, modificar, manter ou transmitir registros eletrônicos devem empregar procedimentos e controles designados a garantir a **autenticidade, integridade** e, quando apropriado, **privacidade** de registros eletrônicos, e a garantir que o signatário **não pode repudiar** o registro assinado como não genuíno. Tais procedimentos devem incluir:*

FDA

- A até D
- E) Uso de trilhas (logs) geradas por computador, seguras e com carimbo de tempo para gravar, independentemente, o dia e a hora de cada entrada do operador para criar, modificar ou excluir registros eletrônicos.
- Mudanças em registros não devem obscurecer informações previamente guardadas
- F a K

FDA

- Para sistemas abertos
  - Mesmo que o anterior, com a adição de cifragem e uso de assinaturas digitais para garantir a autenticidade, integridade e privacidade

FDA

- Manifestações de assinatura
- Devem conter informações que claramente indiquem:
  - Nome do signatário
  - Data e hora da execução da assinatura
  - Significado associado com a assinatura
- Devem preencher os mesmos requisitos dos registros eletrônicos

FDA

- Demais considerações sobre assinatura

Referências

- **FDA CFR 21 Part 11**
- http://www.fda.gov/ora/compliance_ref/part11/FRs/background/pt11finr.pdf

- **Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (RES).**
- http://www.sbis.org.br/GTCERT_20040219_RT_V2.1.pdf

- **Decreto Lei que estabeleu ON - Observatorio Nacional**
- http://www.cenadem.com.br/news_tempestividade.php

- **Página do LabSEC - UFSC**
- http://www.labsec.ufsc.br/

- **BRy - PDDE**
- http://www.bry.com.br/servicos/pdde/testdrive.asp

- **NCipher – pdfProof, DSE 200, TimeSource Server Clock**
- http://www.ncipher.com/timestamping

- **Mykotronx - Fortezza**
- http://www.mykotronx.com/products/fortezza/crypto.asp

- **Verisign - Authentic Document Service**
- http://www.verisign.com/products-services/security-services/code-signing/brew-document-ids/faq.html#01000003

- **Eracom - ProtecServer Orange™**
- http://www.eracom-tech.com/products/pso/pso.htm

- **CRN Brasil**
- www.resellerweb.com.br/noticias/artigo.asp?id=78056

- **A confiança no uso de documentos eletrônicos como fator crítico para o desenvolvimento das organizações modernas**
- www.bry.com.br/painel/palestras/ppt_rolt.ppt