

Segurança Electrónica

(a Solução PKI)

Álvaro Matos
DigitalSign

- Compreender os requisitos de Segurança necessários à Organização
- Saber identificar as técnicas e métodos de ataque mais utilizados
- Compreender os fundamentos de uma PKI
- Compreender a sua necessidade para a garantia da segurança
- Conhecer a legislação aplicável e casos práticos

- **Requisitos de Segurança**

- Confidencialidade
- Autenticação
- Integridade
- Interoperabilidade
- Não repudição

- **Métodos de ataque**

- Ferramentas
- Objectivos e Motivações
- Ataques mais frequentes

- **Infraestrutura de Chave Pública (PKI)**

- Fundamentos da criptografia
- Componentes de uma PKI
- Arquitectura e Organização
- Certificados Digitais
- Listas de Revogação de Certificados (CRLs)
- Assinaturas Digitais

- **Legislação Aplicável**

- **Aplicações e Casos Práticos**

Requisitos de Segurança



- ▶ “By 2004, 80% of enterprises will likely use the Internet as a integral part of their business processes” (Gartner 2001)
- ▶ “Worldwide security products, managed svcs, & PKI prod's will grow 328% from \$5.3B to \$22.7B between 2001 and 2005 (Infonetics Research)
- ▶ “Security budgets will grow as much as 50% per year this decade” (Meta Group 2001)
- ▶ “By 2011, private & gov't spending on data security will grow 10x” (Gartner 2001))

- Security & Privacy
 - “Approximately 60 percent of online adults say security and privacy concerns stop them from doing business on the Web”
- Personal financial information
 - “Eighty-six percent of online American adults are very concerned about the security of bank and brokerage account numbers when doing online transactions. 83 percent, expressed the same concerns about the security of their Social Security and credit card numbers. Additionally, 70 percent are very concerned about the security of their personal information, including their income and assets, according to Gartner.”
- GartnerG2 research analyst Laura Behrens
 - “Even though many consumers say they're uncomfortable sharing information on the Web, for the right combination of convenience or reward, many go ahead and share anyway.”

Gartner

CSI/FBI 2000 Computer Crime & Security Survey

- Total = 265,589,940
 - Numbers are based on total losses incurred from data lost, fraud or abuse of 273 respondents
- Unauthorised Insider Access
 - 22,544,500 US\$
- Theft of Proprietary Information
 - 66,708,000 US\$
- Telecom Fraud
 - 4,028,000 US\$
- Financial Fraud
 - 55,996,000 US\$
- Virus Attacks
 - 29,171,700 US\$
- Laptop Theft
 - 10,404,300 US\$
- Insider Network Abuse
 - 27,984,740 US\$
- Denial of Service
 - 8,247,500 US\$
- Sabotage
 - 27,148,000 US\$
- System Penetration
 - 7,104,000 US\$
- Telecom Eavesdropping
 - 991,200 US\$
- Active Wiretapping
 - 5,000,000 US\$



John Hancock



Confidencialidade

autenticação

Integridade

Interoperabilidade

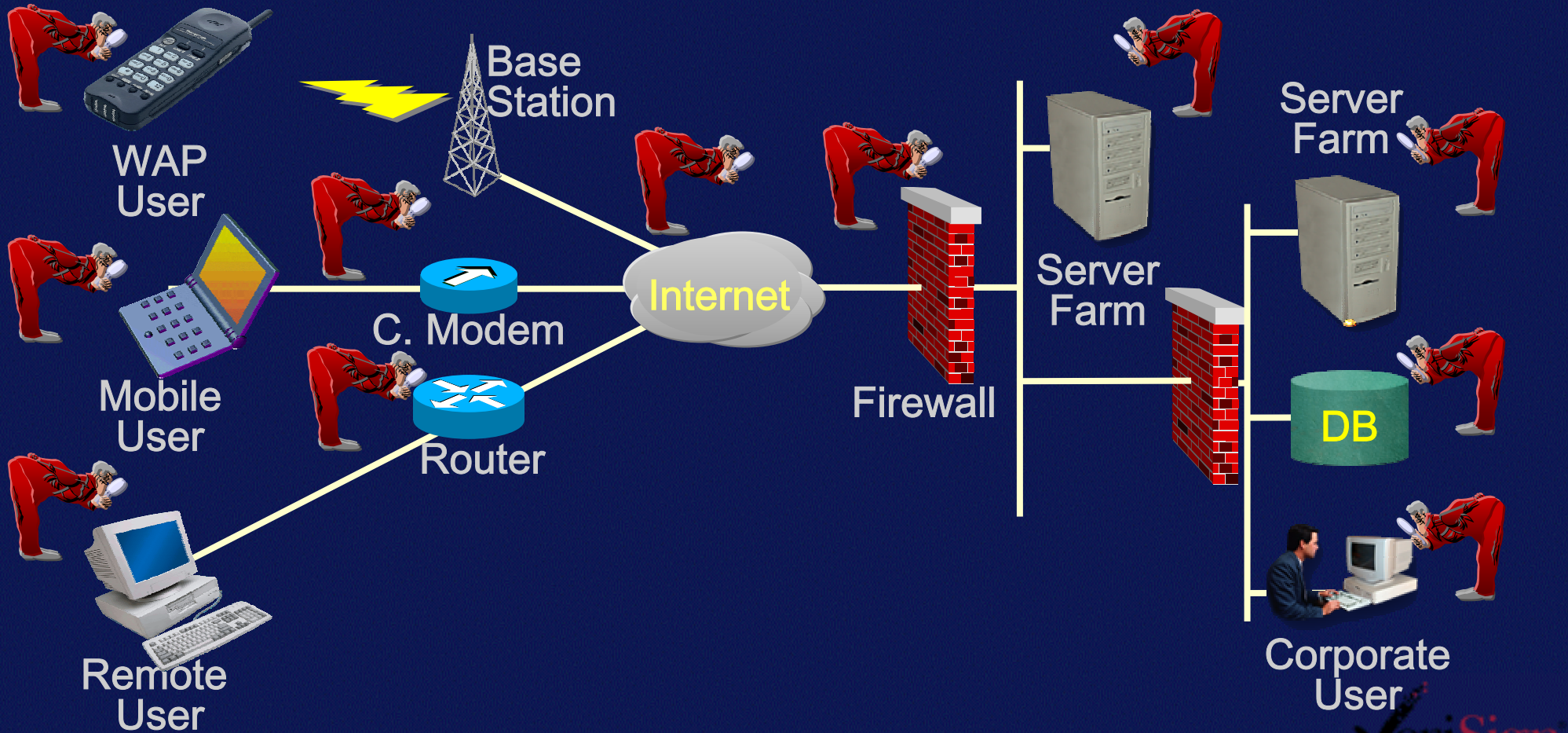
Não-Repudição



Digital Signature



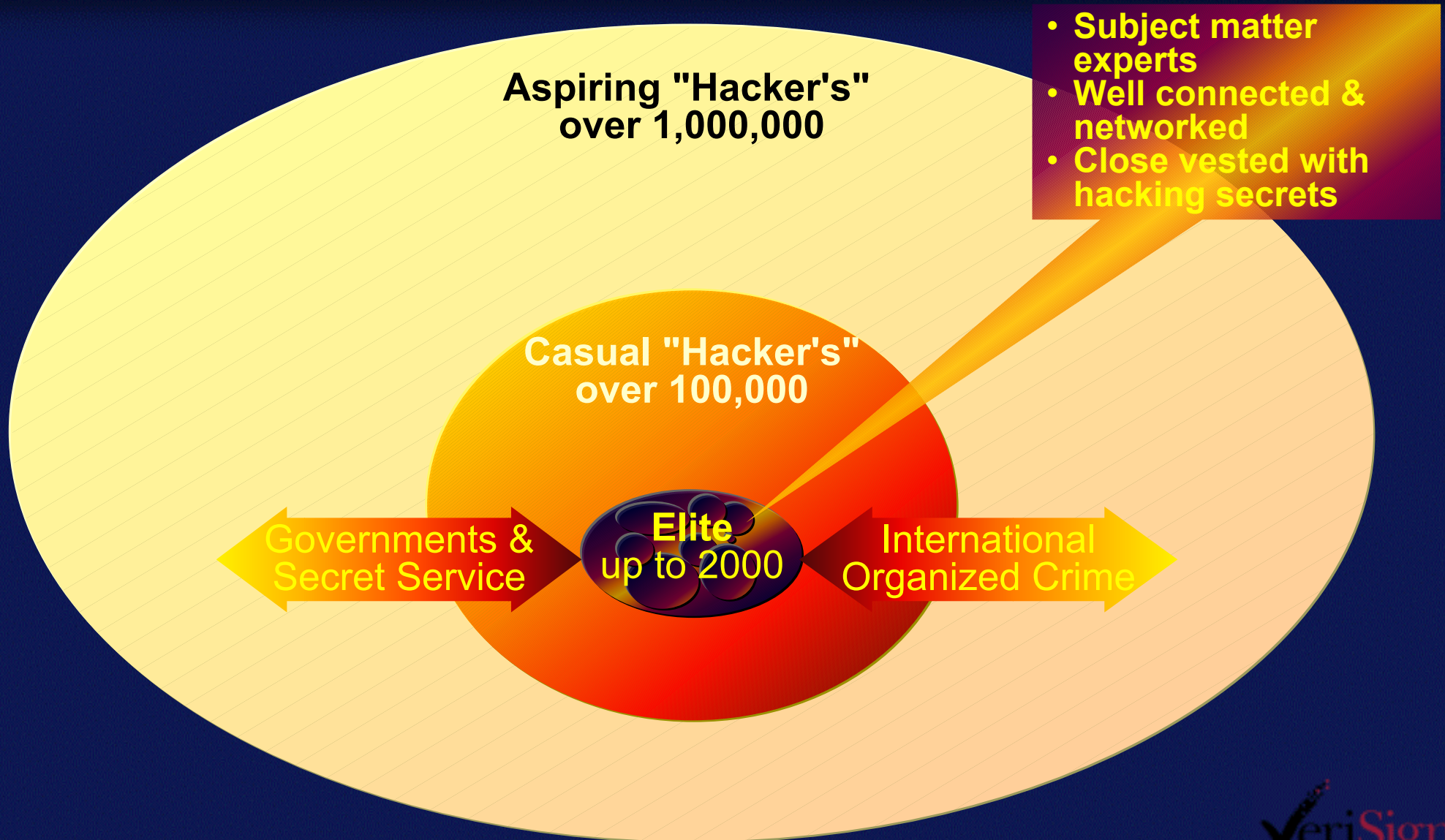
Métodos de Ataque



- Laboratórios multi-plataforma em rede como base
 - Todos os Sistemas Operativos são conhecidos e disponíveis no mercado
 - Grande número de vírus e scripts de ataque disponíveis
- Ferramentas de exploração & ataque
 - Ataques *Denial Of Service* & *Brute Force*
 - *Mail Bombs*, *Stealth Tools*, *ICMP Flooding*, etc.
- Dispositivos de *Eaves Dropping* & *Sniffing*
- *Password Cracking*
 - Dicionários multi-língua
- RAS (Remote Access Server) & Back Door WarDialers
- As ferramentas de *Hacking* estão normalmente disponíveis na Net



**looking for
Information
Leaks**



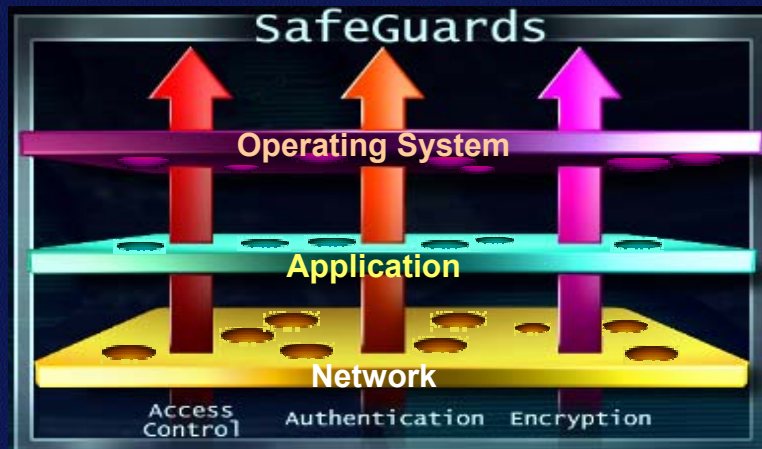
- Objectivo:
 - “ser root” – Obter privilégios máximos
 - “controlar” o sistema
- Motivações
 - Aceder a recursos que supostamente privados ou restritos
 - Demonstrar habilidades técnicas – depois “gabar-se”
 - Fama, status, vingança, política, ...
- Métodos:
 - Explorar *loopholes*
 - Explorar falhas nas configurações
 - Auditorias a protocolos
 - Explorar Erros Humanos

▪ Spoofing

- O atacante usa a identificação de outro, fazendo-se passar por essa pessoa ou dispositivo

▪ Session Hijacking

- O atacante “rouba” uma ligação existente entre duas máquinas



▪ Sniffing

- Um sniffer pode registrar todo o tráfego existente na rede para posterior análise

▪ Man-in-the-Middle

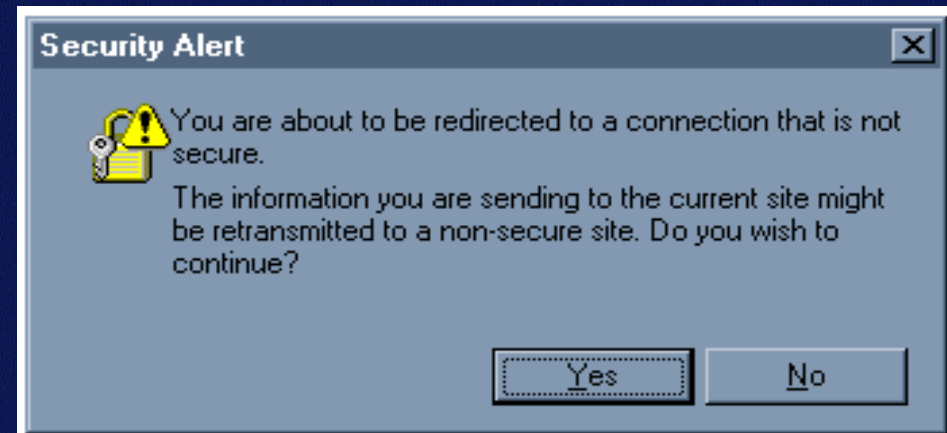
- Um atacante sofisticado utilizando spoofing, hijacking ou sniffing pode “colocar-se no meio” de uma sessão de troca de chaves – ou até utilizar as suas próprias chaves

▪ Phishing & Trojans

- Envio de informação enganosa com o intuito de obter dados confidenciais ou instalação de aplicações maliciosas

- 75% dos ataques bem sucedidos nunca chegam a ser descobertos!

- A grande maioria dos ataques têm origem dentro da Organização
- Funcionários maldosos podem monitorar, alterar, reencaminhar pacotes de informação, etc.



Infraestrutura de Chave Pública (PKI)

- Segurança em canais fechados

baseia-se no *obscurantismo* nas *comunicações* e nas técnicas: o conhecimento sobre o tráfego de informação e sobre as técnicas de segurança é controlado



- Os sistemas de segurança, uma vez instalados, não são testados e se forem atacados não é fácil constatar a existência e a natureza do ataque

MUITO GRAVE!!!



- Não impõe requisitos especiais aos sistemas computacionais

- Segurança em canais abertos

assume que todo o tráfego de informação é público e que as técnicas de segurança são publicamente conhecidas. O controlo do segredo restringe-se a certos itens de informação: **as chaves**



- Os sistemas de segurança podem ser testados pela comunidade científica em geral e eventuais quebras de segurança têm mais possibilidades de ser detectadas



- Porque o conhecimento dos intrusos é maior, as técnicas de segurança devem ser mais exigentes e computacionalmente mais elaboradas do que as usadas em canais fechados

POUCO GRAVE!!!

- A mesma chave é utilizada para cifrar e para decifrar as mensagens
- A chave é partilhada pelos intervenientes na comunicação
- Funcionamento:
 - Miguel tem uma chave secreta.
 - Joana quer enviar uma mensagem confidencial:
 - Miguel envia a chave à Joana.
 - Joana cifra a mensagem com a chave do Miguel.
 - Miguel decifra a mensagem com a chave.

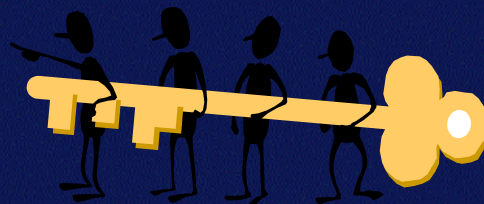


■ Vantagens:

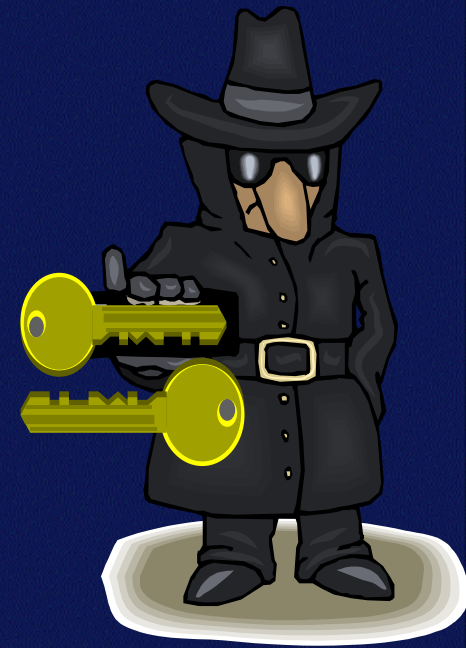
- Não necessita de qualquer infraestrutura de segurança
- Simplicidade computacional

■ Desvantagens:

- Distribuição das chaves
- Necessidade de guardar $N-1$ chaves



- Cada utilizador possui 2 (duas) chaves complementares:
 - Privada: do exclusivo conhecimento do seu detentor
 - Pública: do conhecimento público (partilhada)
- Funcionamento:
 - O Miguel possui 2 chaves (pública e privada).
 - Joana quer enviar uma mensagem confidencial:
 - Joana obtém a chave pública do Miguel.
 - Joana cifra a mensagem com a chave do pública Miguel.
 - Miguel decifra a mensagem com a sua chave privada.



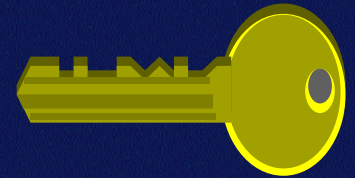
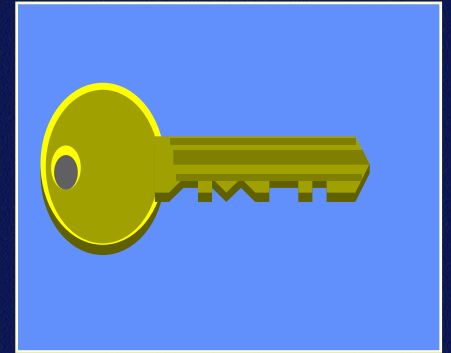
■ Vantagens:

- Distribuição de chaves
- Segredo não compartilhado
- Apenas é necessário guardar uma chave

■ Desvantagens:

- Como saber a quem pertence a chave pública

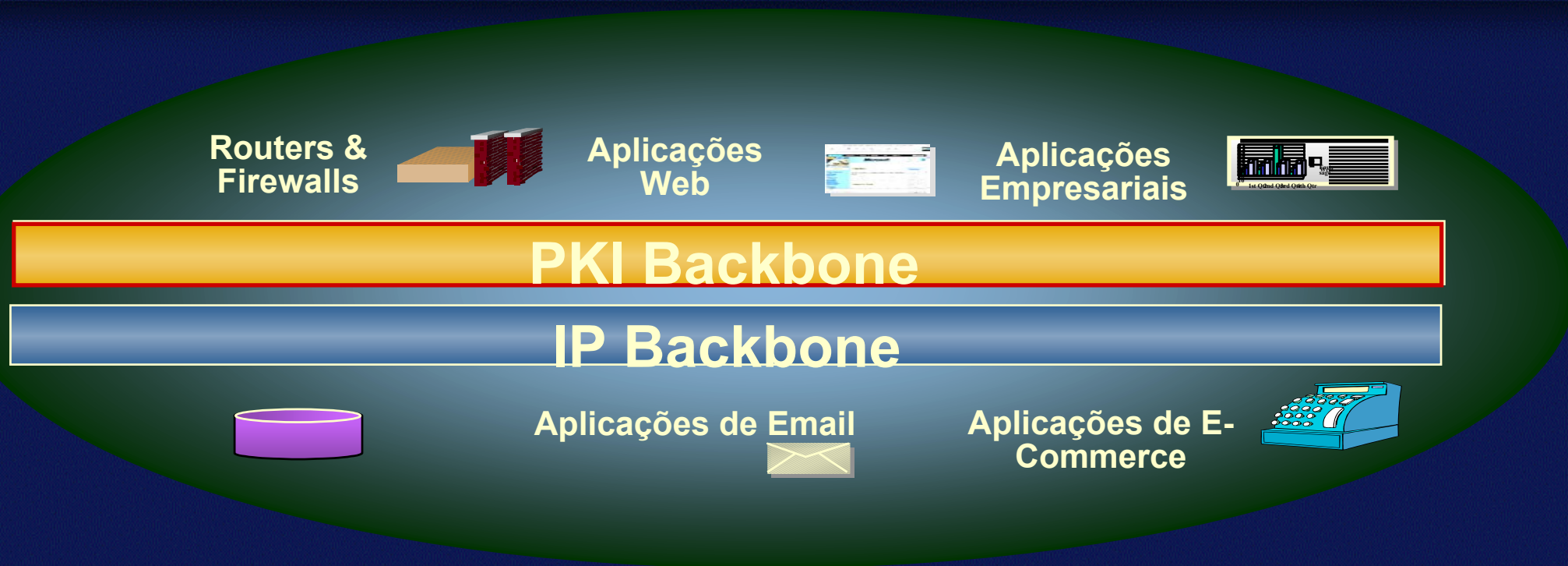
PRIVADA



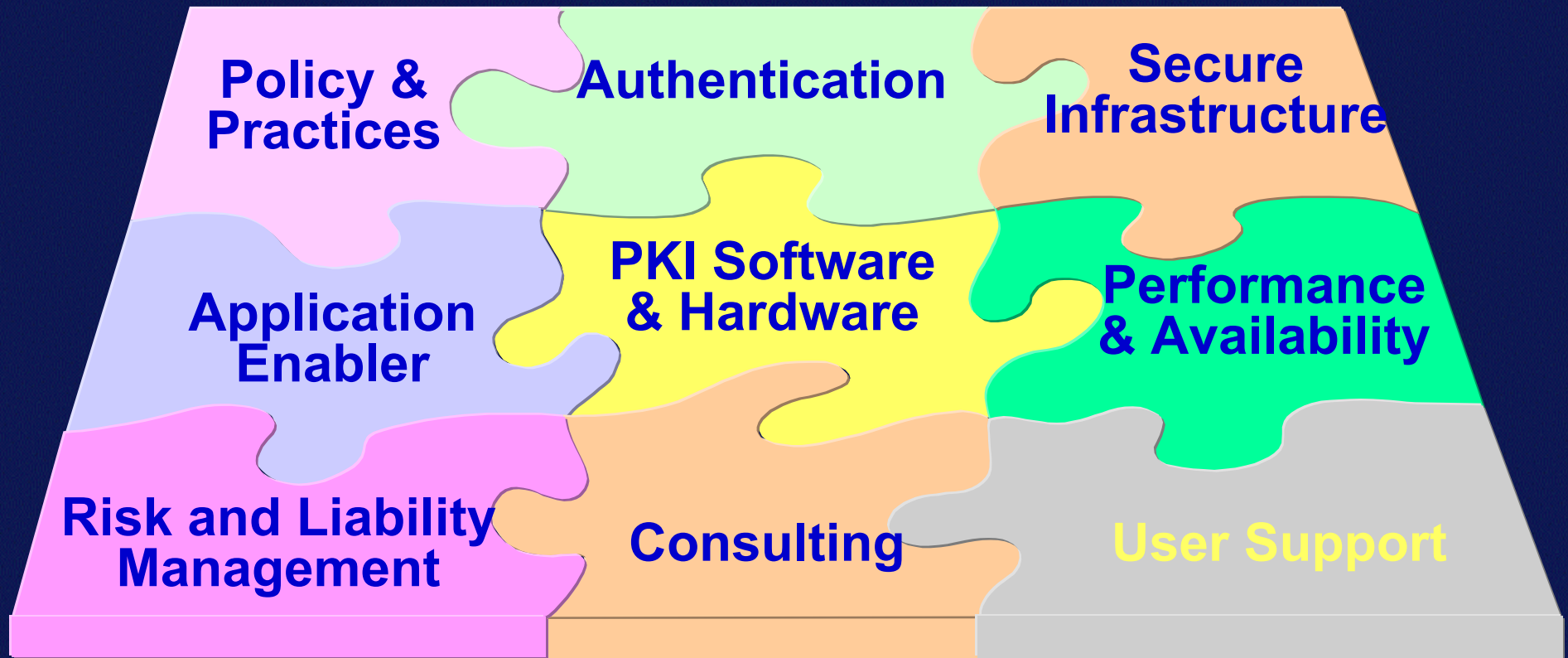
PUBLICA

- Solução \Rightarrow Infraestrutura de Chave Pública (PKI)

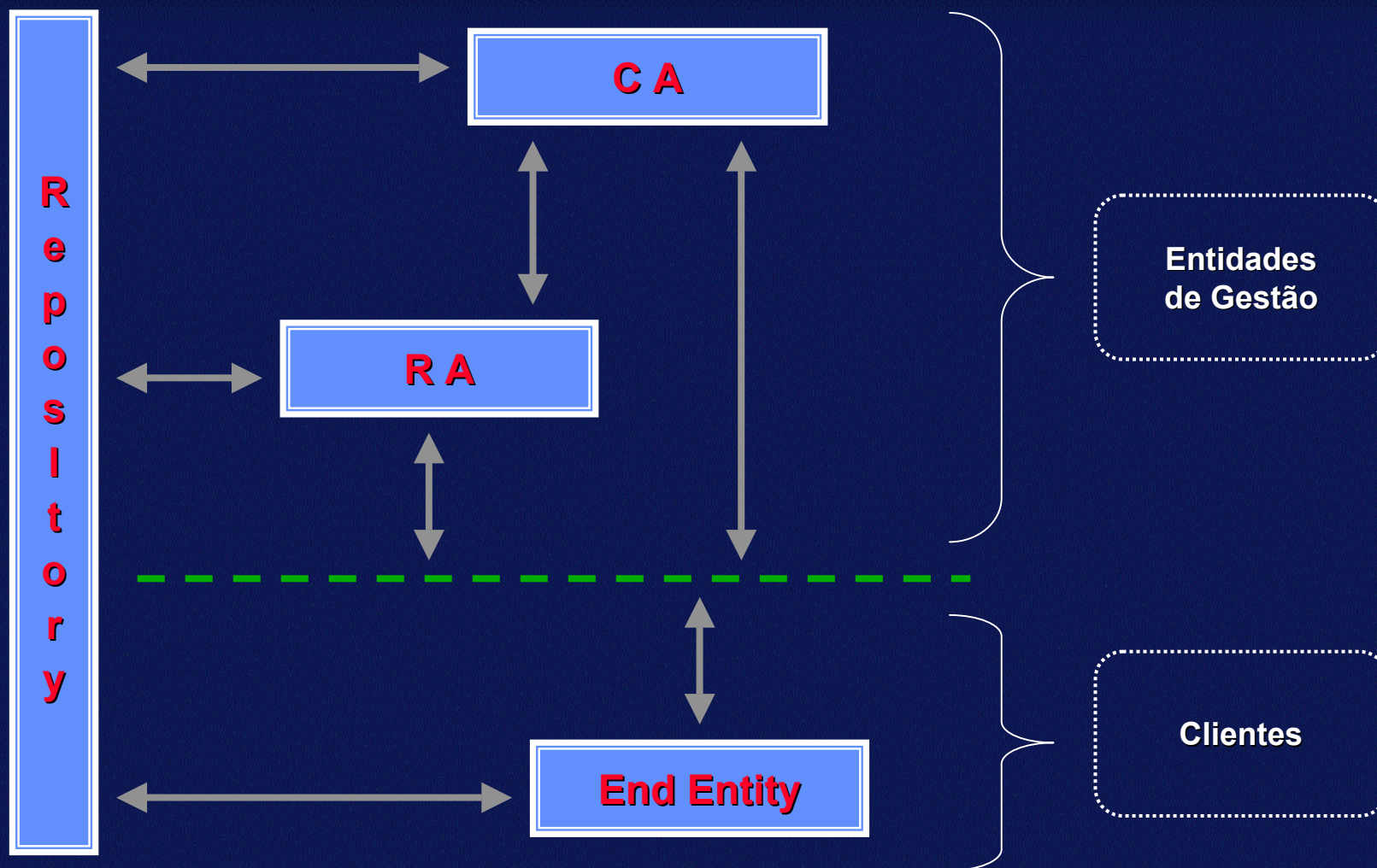
Infraestrutura de Chave Pública (PKI)



PKI é, basicamente, um conjunto de hardware, software, pessoas, políticas e procedimentos necessários para criar, gerir, armazenar, distribuir, e revogar certificados baseados na criptografia de chave pública



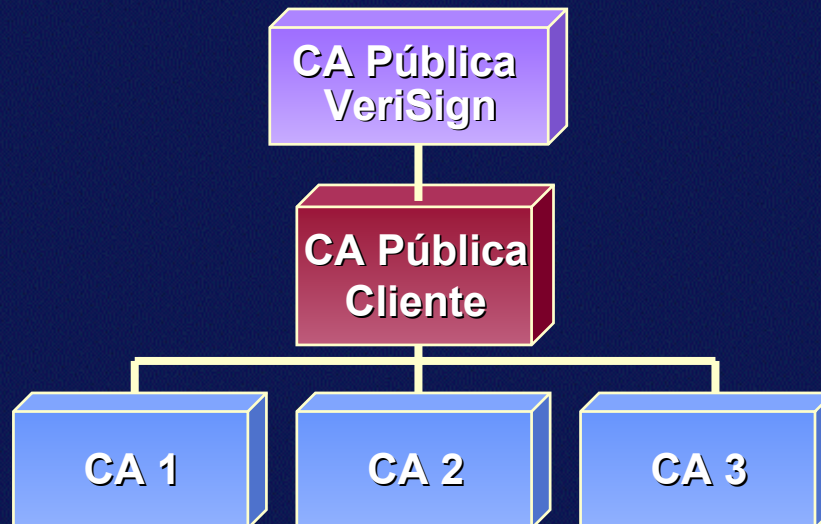
A tecnologia é apenas um dos componentes da PKI





Comunidade Fechada

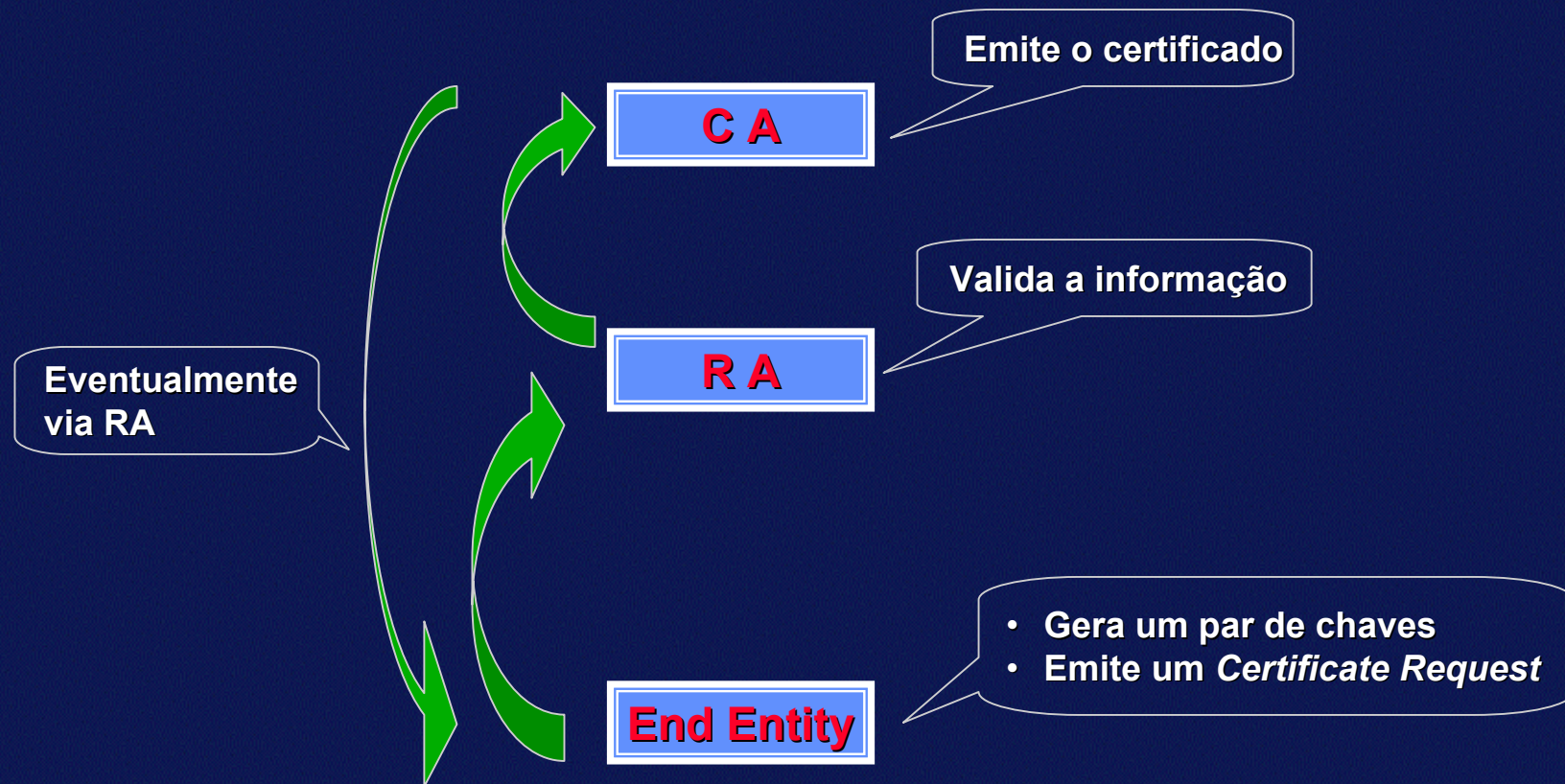
- Acesso à Rede
- B2B privado



Comunidade Aberta

- E-Mail Seguro
- Aplicações Web

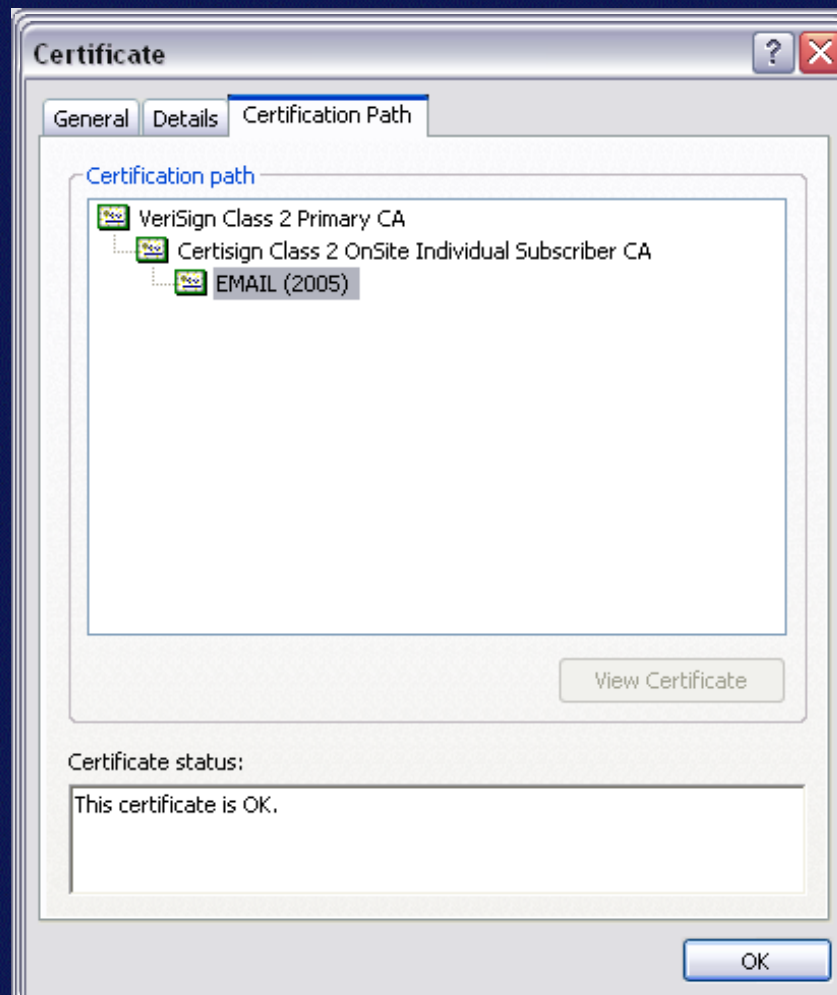
Pedido de certificados (passos típicos)

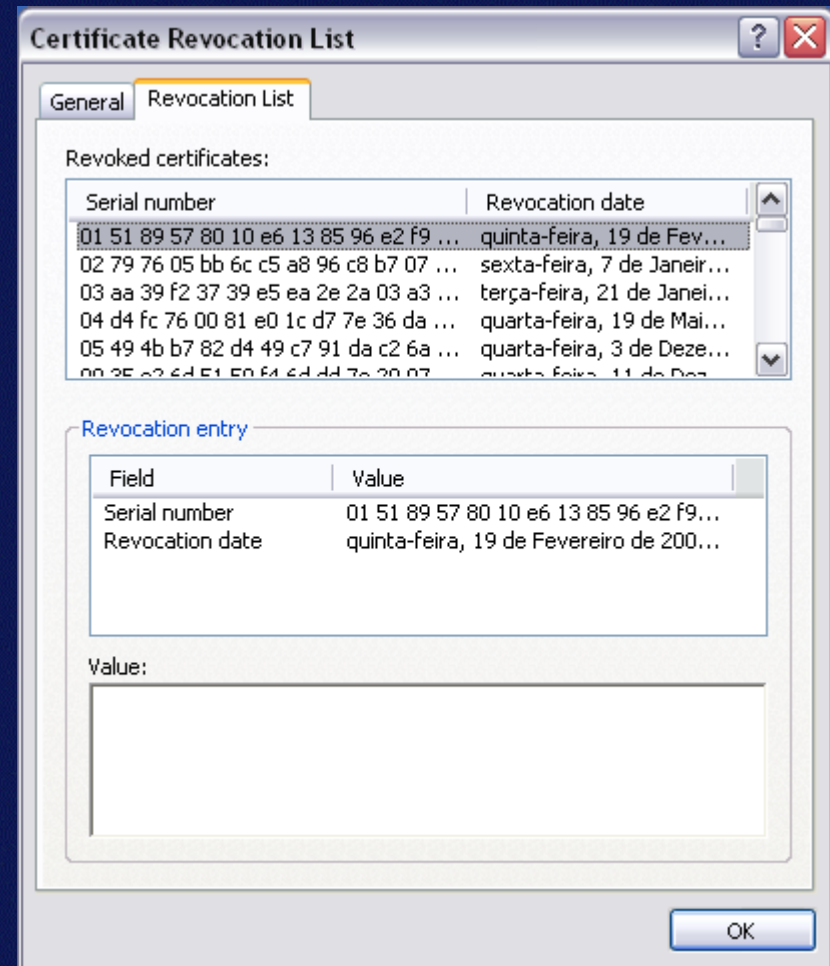
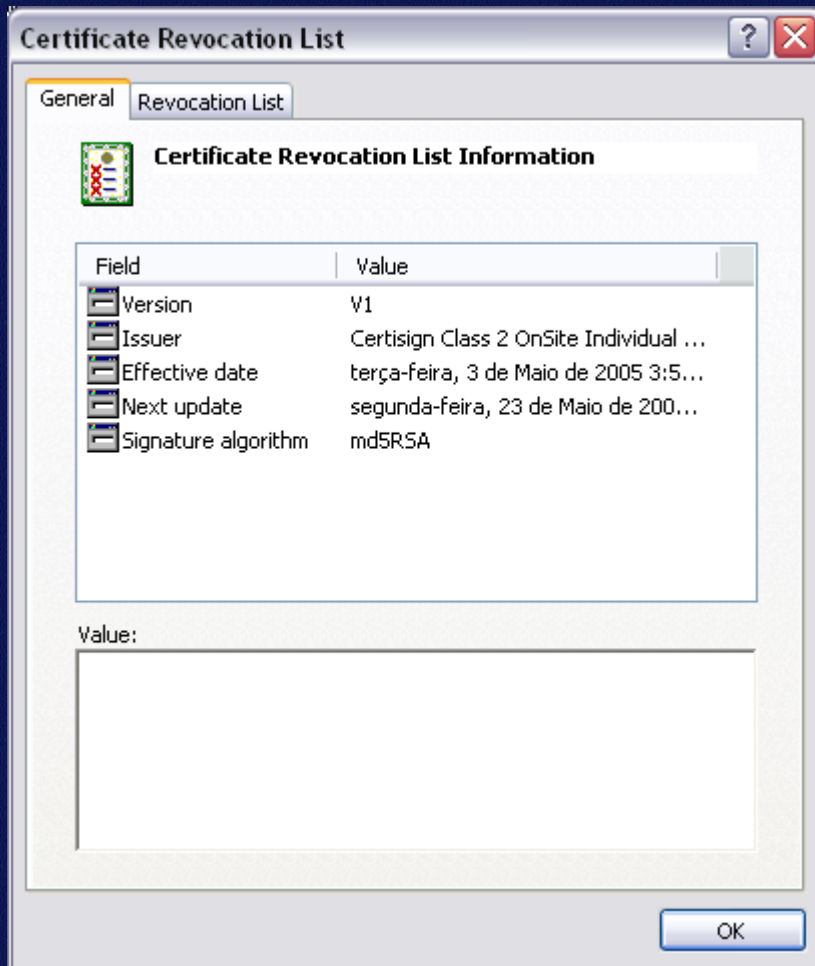


Conteúdo de um certificado digital

| |
|---------------------------|
| Versão |
| Número de série |
| Entidade emissora (CA) |
| Validade |
| Detentor (subject) |
| Chave pública do detentor |
| Extensões |

Conteúdo de um certificado digital





▪ Definição:

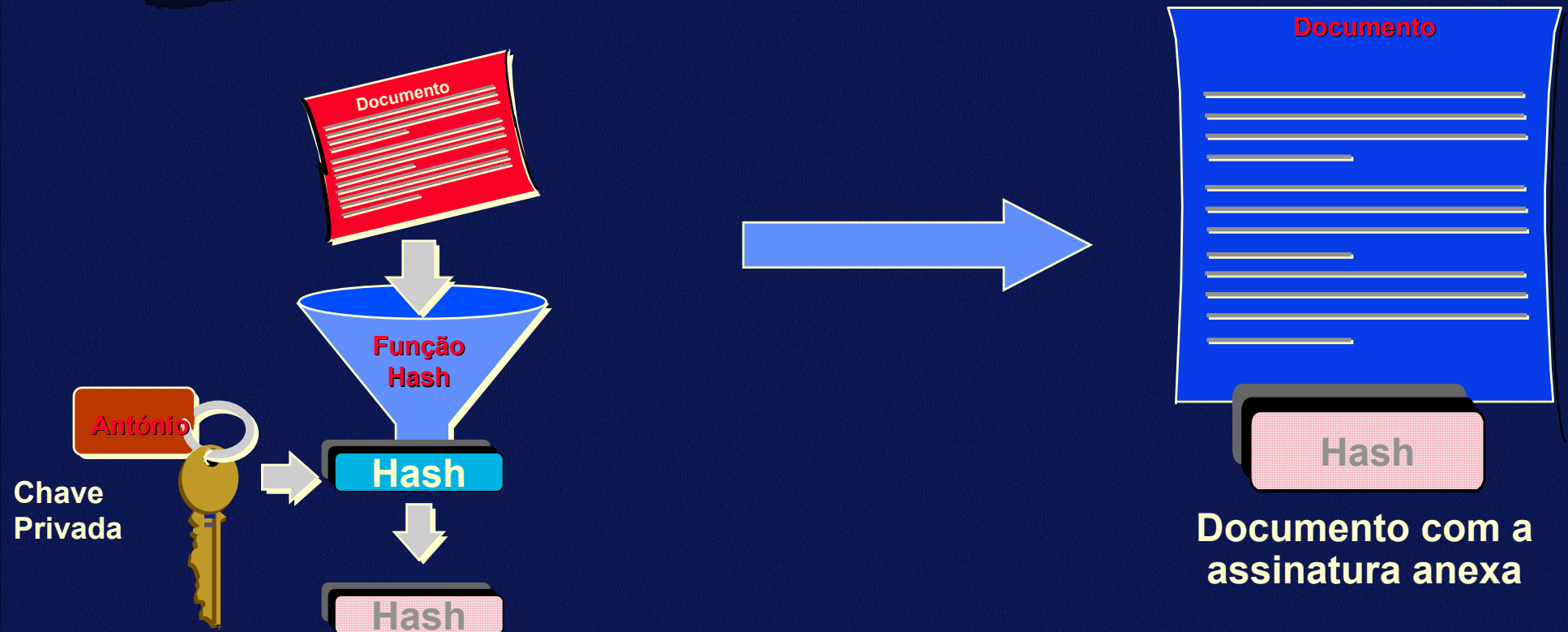
Uma Assinatura Digital (não confundir com Certificado Digital) é um documento electrónico que atesta identidade do assinante.

▪ Propriedades

- Autenticação
- Não repudição
- Verificação de integridade do documento

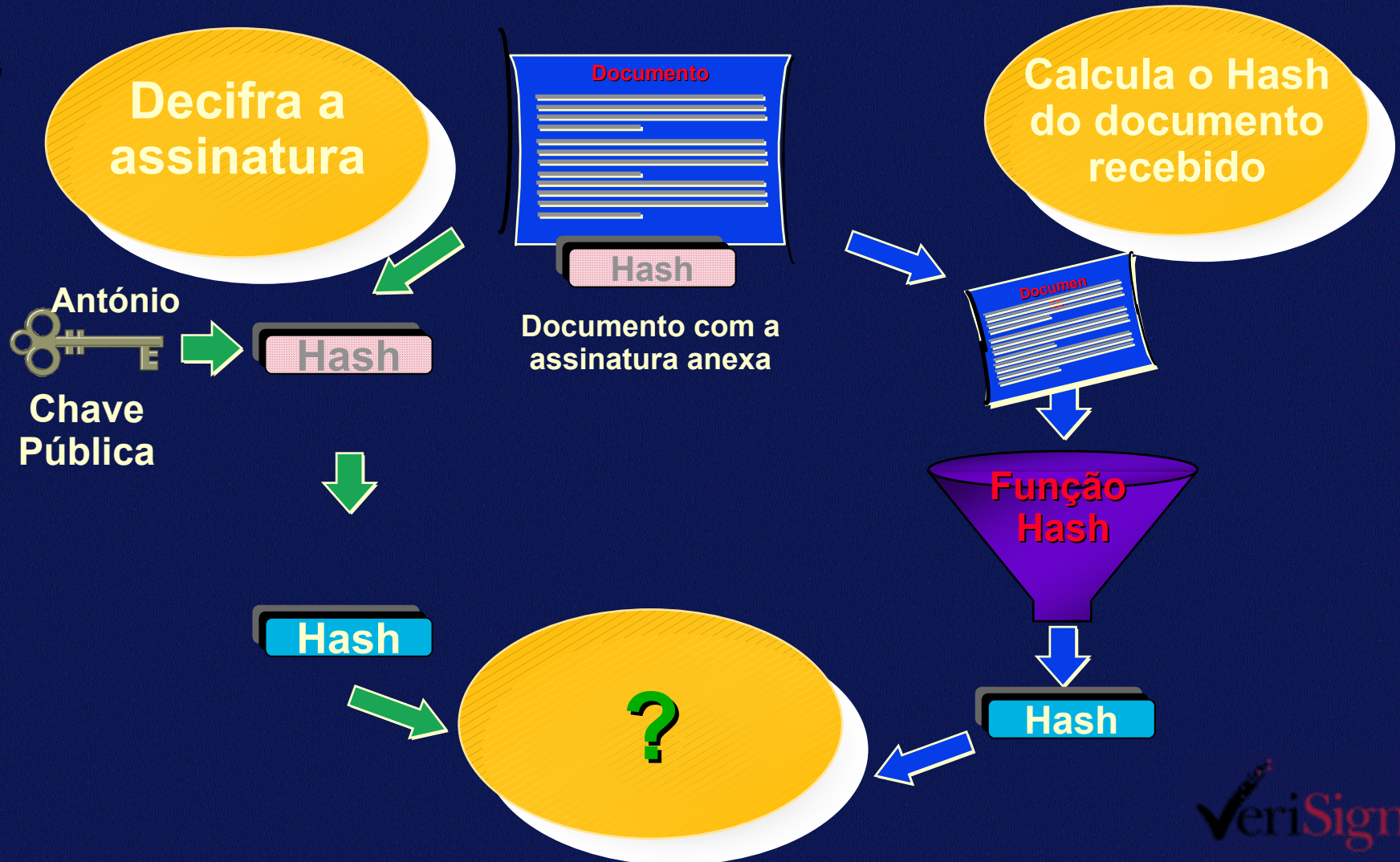
António

Criação da Assinatura Digital

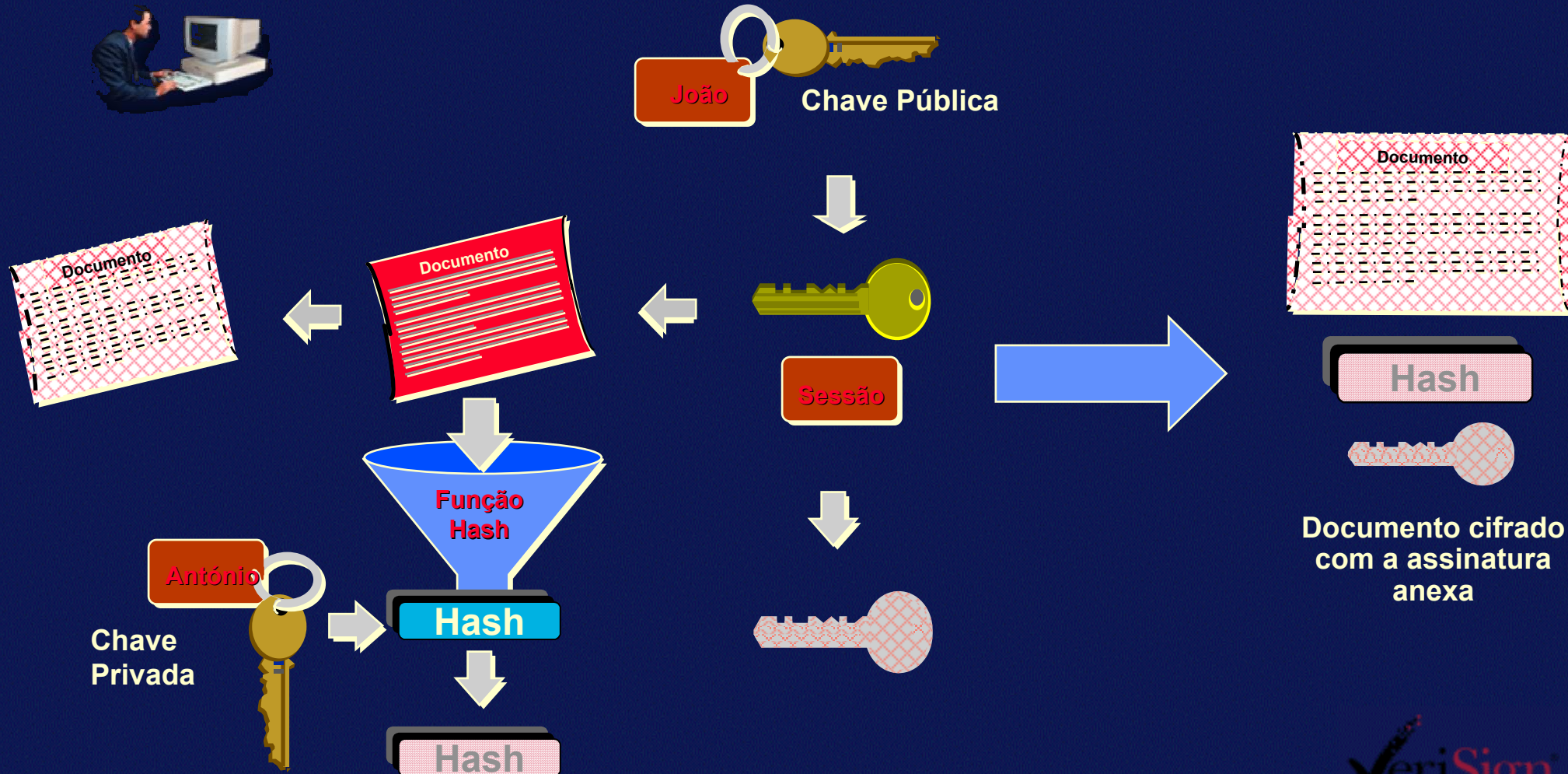


João

Verificação da Assinatura Digital



António Criação da Assinatura Digital + Cifra

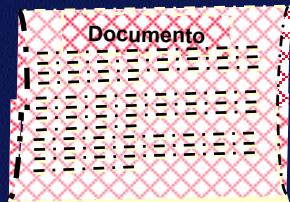


João

Verificação da Assinatura Digital + Cifra



Documento cifrado com a assinatura anexa



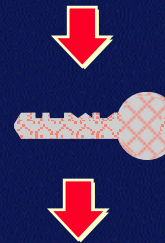
João
Chave Privada

Decifra a chave de sessão

Calcula o Hash do documento recebido

Decifra a assinatura

António
Chave Pública



- **Segredo não partilhado**
A chave privada é do exclusivo conhecimento do seu detentor.
- **Simplicidade na distribuição de chaves**
A chave pública é incluída no certificado, que é do conhecimento público.
- **Simplicidade no manuseamento das chaves**
Apenas precisa de guardar uma chave
- **Reconhecimento a nível global**
Com a inclusão da entidade de confiança (CA)

Legislação Aplicável

- Em Portugal, a assinatura digital foi instituída pelo decreto lei 290-D/99, de 2 de Agosto, com as alterações introduzidas pelo decreto lei 62/2003, de 3 de Abril, como um processo de assinatura electrónica baseado em sistema criptográfico assimétrico
- A aposição de uma assinatura digital a um documento electrónico equivale à assinatura autografa dos documentos com forma escrita sobre suporte de papel e cria a presunção de que:
 - a) a pessoa que após a assinatura digital é o titular único e exclusivo desta;
 - b) a assinatura digital foi aposta com a intenção de assinar o documento electrónico;
 - c) o documento electrónico não sofreu alteração desde que lhe foi aposta a assinatura digital, sempre que seja utilizada para verificação uma chave pública contida em certificado válido emitido por entidade certificadora.

- Dec-Lei 256/2003 - Transpõe para a ordem jurídica nacional a Directiva 2001/115/CE
- Entrou em vigor em 1 de Janeiro de 2004
- Até 31 de Dezembro de 2005, a utilização da factura electrónica está apenas condicionada à prévia comunicação à Direcção-Geral dos Impostos [Art.º 7º]
- As facturas electrónicas ou documentos equivalentes podem, sob reserva de aceitação pelo destinatário, ser emitidas por via electrónica, desde que seja garantida a autenticidade da sua origem e a integridade do seu conteúdo, mediante assinatura electrónica avançada [Art.º 35º]

- Aguarda-se a Criação de uma *Root CA* pelo Governo
- Legislação sobre Autoridades Certificadoras já completa
- A Justiça com a Certificação Digital de Juízes e Funcionários (ITIJ) e Advogados (Ordem dos Advogados) é um caso de sucesso na desmaterialização dos processos, com segurança
- A DigitalSign espera nos próximos meses concluir o seu processo de acreditação

Aplicações Práticas



Os documentos podem *desaparecer*



Existem *backups*?!



É possível falsificar documentos



Muitos processos importantes permanecem no papel

A *digitalização* de documentos sem recurso à Assinatura Digital não traz qualquer segurança - a **integridade** e a **autenticidade** não são garantidas

-----Mensagem original-----

De: Citibank [mailto:antifraud_department.ref.num8801@citibank.com]

Enviada: segunda-feira, 25 de Outubro de 2004 13:00

Para: fmoreira@certisign.pt

Assunto: CITIBANK: URGENT SECURITY NOTIFICATION FOR ALL CLIENTS



Dear CitiBank customer,

Recently there have been a large number of identity theft attempts targeting CitiBank customers. In order to safeguard your account, we require that you confirm your banking details.

This process is mandatory, and if not completed within the nearest time your account may be subject to temporary suspension.

To securely confirm your Citibank account details please go to:

https://web.da-us.citibank.com/signin/scripts/login/confirm/user_data.jsp

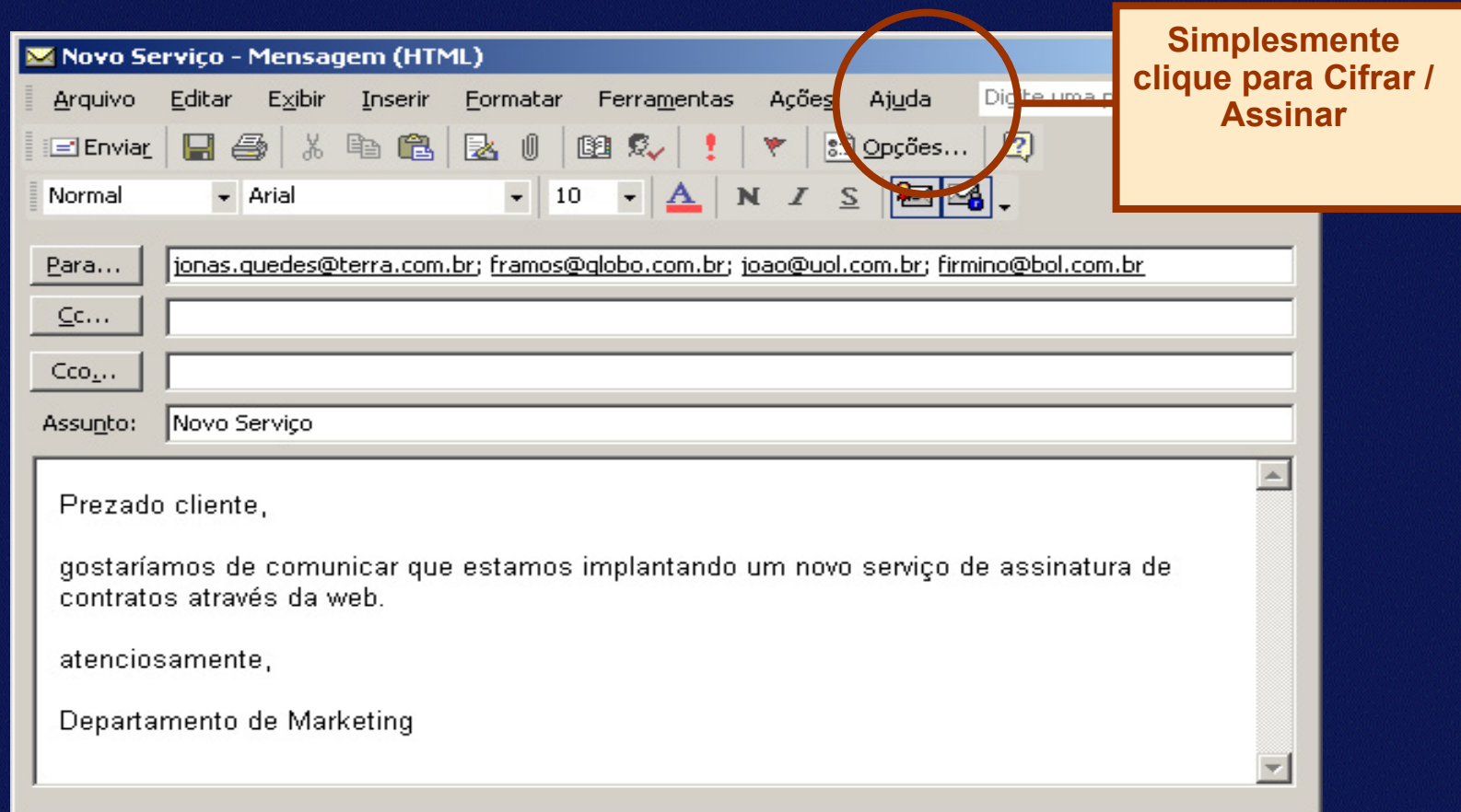
Thank you for your prompt attention to this matter and thank you for using CitiBank!

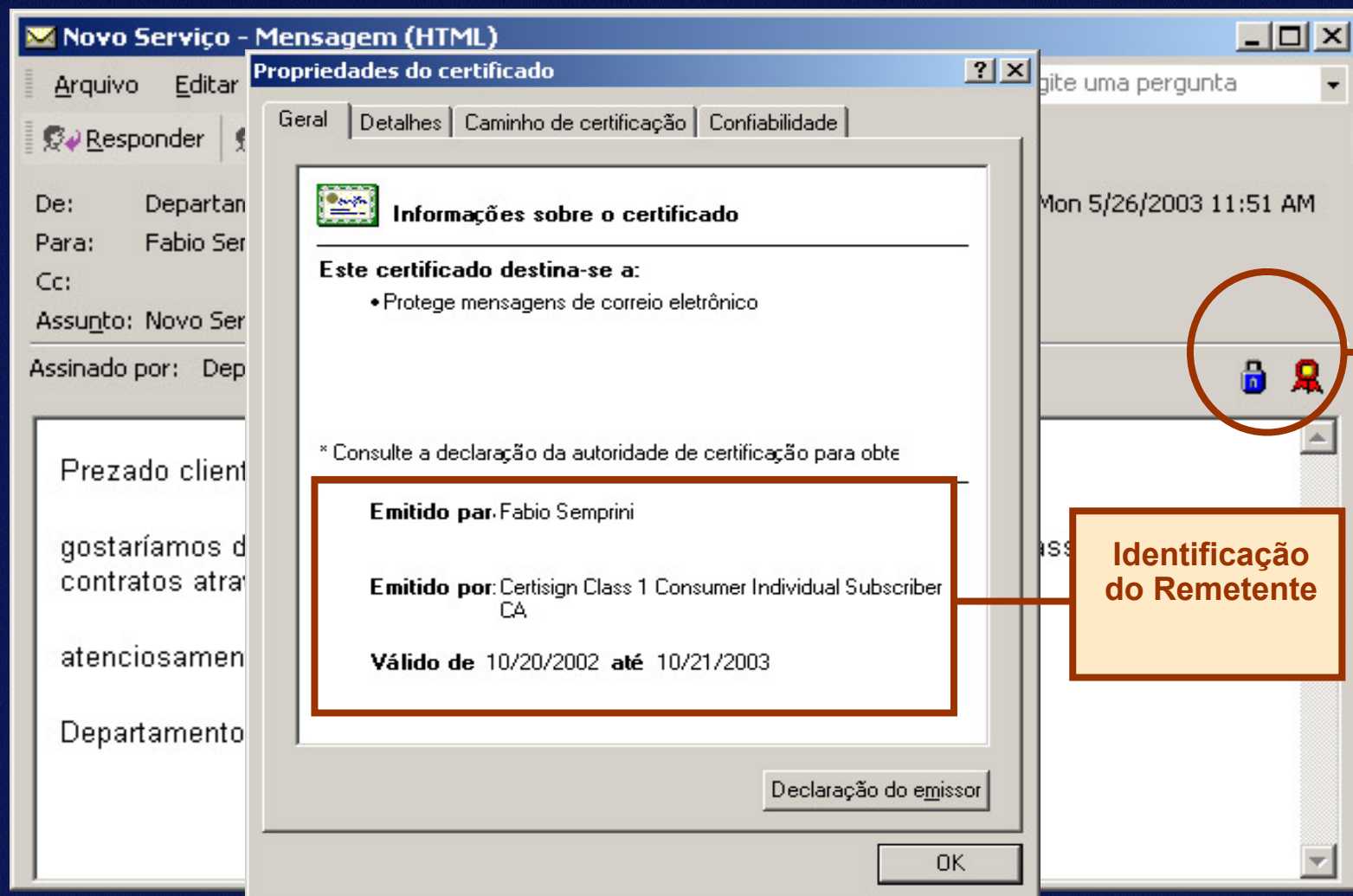
Citi® Identity Theft Solutions

Do not reply to this email as it is an unmonitored alias

A member of citigroup
Copyright © 2004 Citicorp

- A solução passa pela utilização de correio seguro!

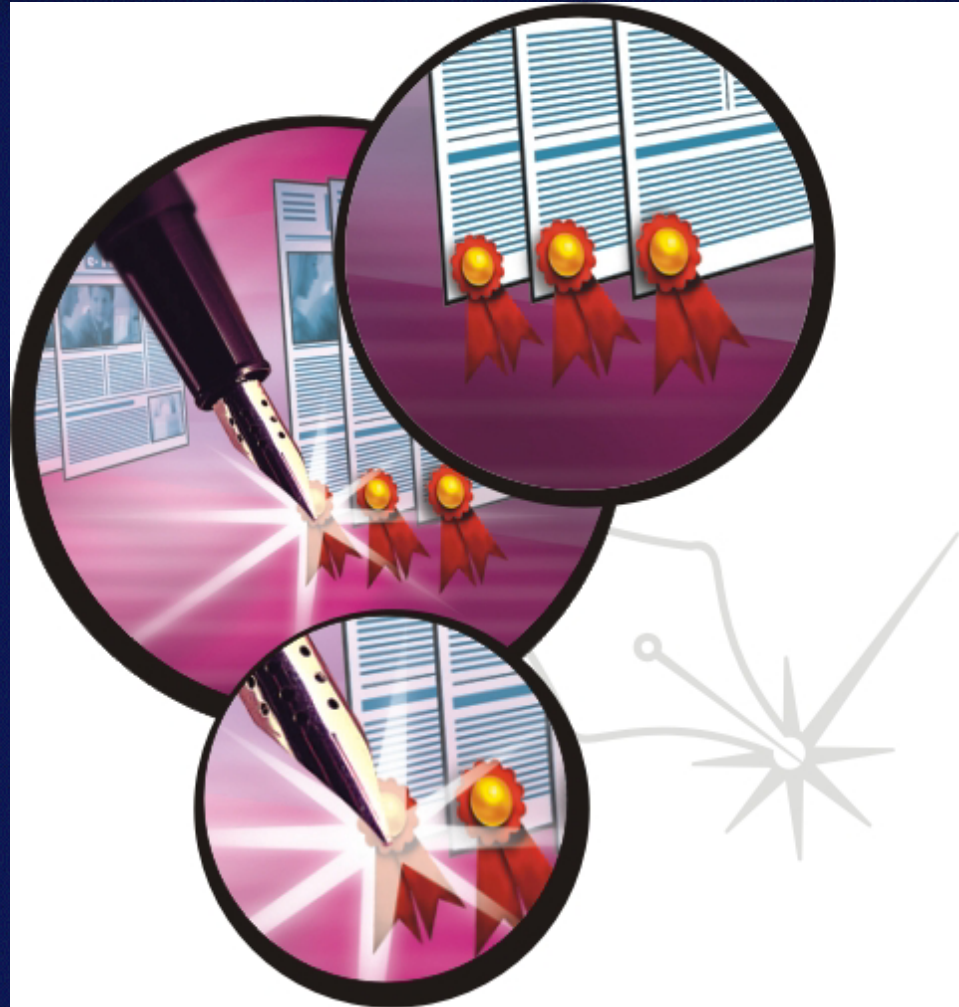




Garantia de
Confidencialidade e
Integridade

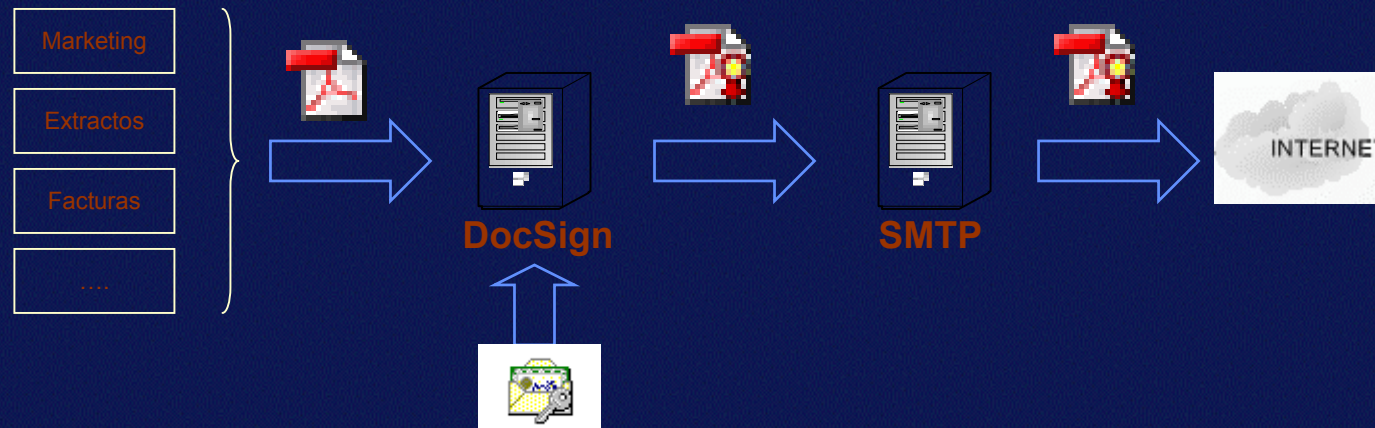
Identificação
do Remetente

- Assina Digitalmente, Facturas Eletrónicas, Extractos Etc.
- Previne ataques de Phishing e Scam.
- Aplicação pode ser implantada em qualquer plataforma (100% Java)



Como funciona?

- Recebe documentos em formato PDF (facturas, extractos, etc.)
- Assina digitalmente esses documentos
- Envia os documentos assinados ao cliente
- Gestão *web-based*



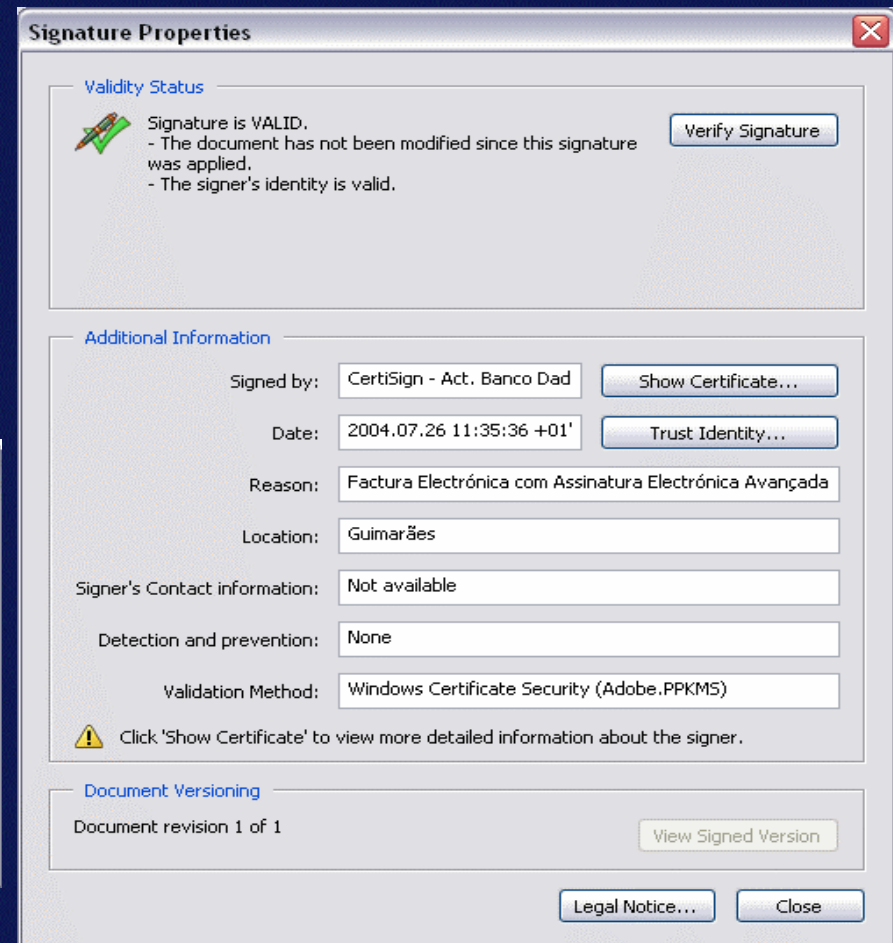
Verificando a Assinatura Digital

| | |
|---------------|--------|
| Total (EUR) | 833,00 |
|---------------|--------|



Factura Electrónica com Assinatura Electrónica Avançada
Guimarães, 26-07-2004

N. 39 R/C- 4810-737 Nespereira GMR - Tel.:253.500642 Fax:253.500639
 do Registo Comercial de Guimarães sob o n.º 8306 Cont. n.º 504005080



➤ Funcionalidades:

- **Identificação:** Mostrando o cartão, ou inserindo-o num qualquer leitor, deverá ser possível obter a informação constante do cartão (à excepção das chaves), e ter a possibilidade de confirmar a integridade e autenticidade da mesma
- **Autenticação:** através da utilização do certificado e respectiva chave privada, aliada ao número da atribuído pelo serviço ao qual se deseja identificar, seria possível a qualquer indivíduo comprovar a sua identidade perante tal serviço, seja de uma forma on-line mas também garantindo as mesmas funcionalidades aquando da impossibilidade de ligação aos serviços centrais
- **Assinatura Digital:** Através do uso do PIN e do certificado digital de assinatura, seria possível a qualquer cidadão (eventualmente apenas a partir da maioridade) assinar mensagens de correio electrónico, documentos nos mais diversos formatos (PDF, Word, XML, etc.), formulários web, etc., com o mesmo valor legal que uma assinatura autografa, de acordo com a legislação em vigor

➤ Aplicações práticas:

➤ Identificação e Autenticação:

- Serviços públicos centrais e locais de acesso web (portais)
- Banca electrónica
- Voto electrónico
- Receita electrónica
- ...

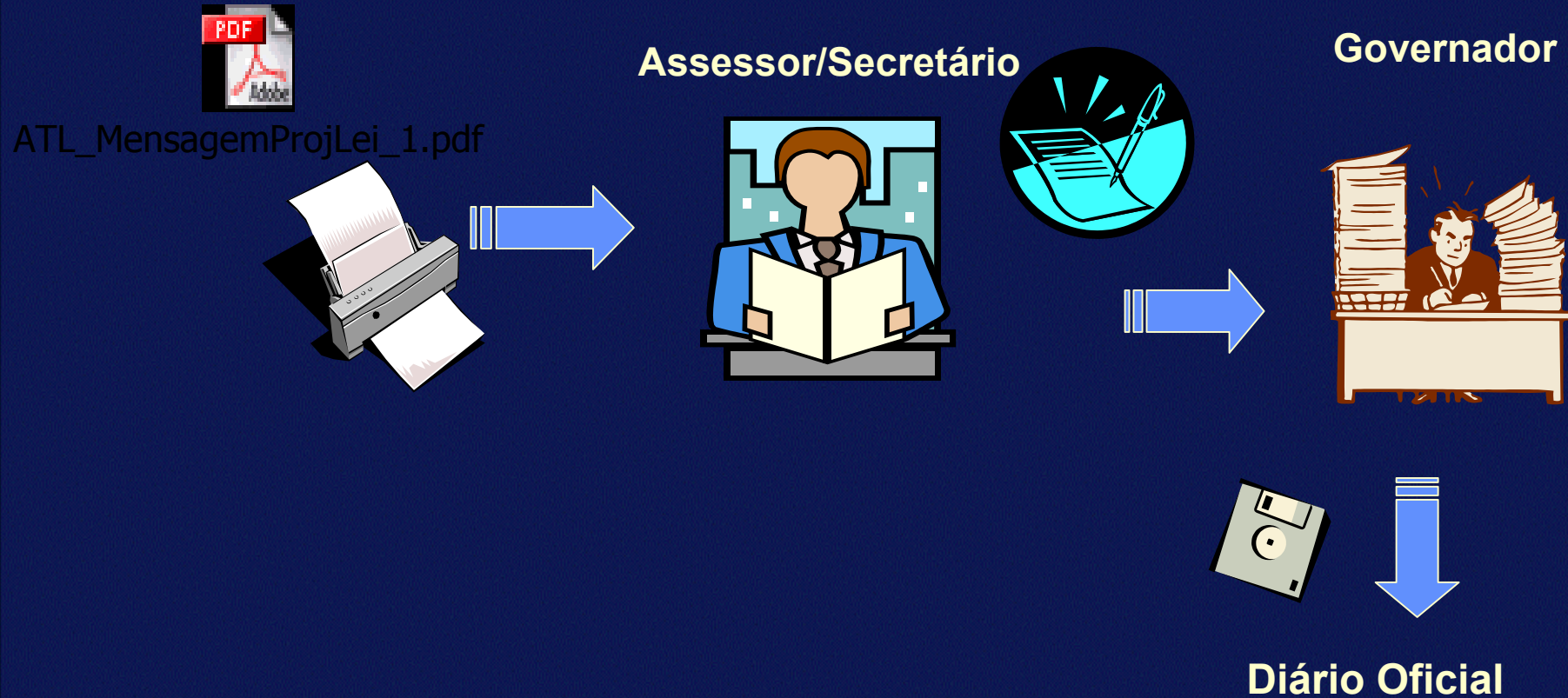
➤ Assinatura Digital:

- Entrega de declarações (IRS, IRC, IVA, etc)
- Facturação electrónica
- Correio electrónico seguro
- Geração de certidões por parte dos serviços públicos
- ...

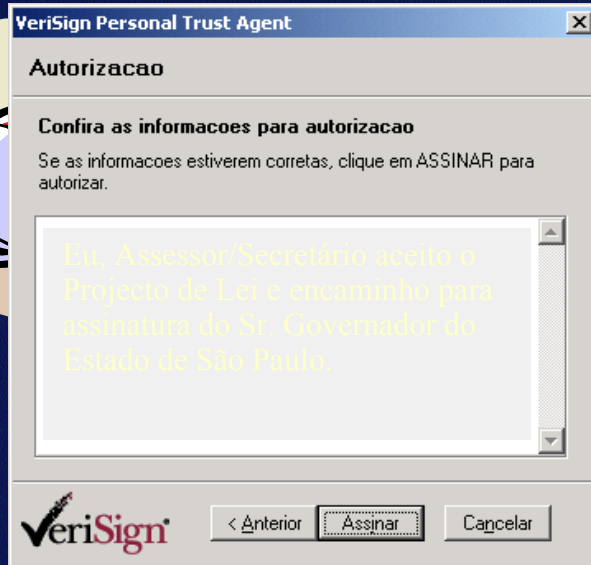
➤ Bélgica:



- Actualmente com mais de 55.000 cartões emitidos
- Até final de 2009, todos os cidadãos Belgas e imigrantes residentes terão um cartão de identificação electrónico



Assessor/Secretário



VeriSign Personal Trust Agent

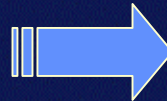
Autorizacao

Confira as informacoes para autorizacao
Se as informacoes estiverem corretas, clique em ASSINAR para autorizar.

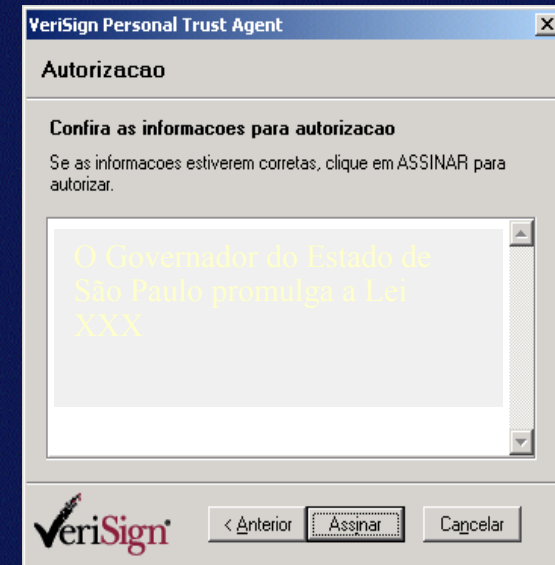
Eu, Assessor/Secretário aceito o Projecto de Lei e encaminho para assinatura do Sr. Governador do Estado de São Paulo.

VeriSign® < Anterior Assinar Cancelar

Intranet



Governador

VeriSign Personal Trust Agent

Autorizacao

Confira as informacoes para autorizacao
Se as informacoes estiverem corretas, clique em ASSINAR para autorizar.

O Governador do Estado de São Paulo promulga a Lei XXX.

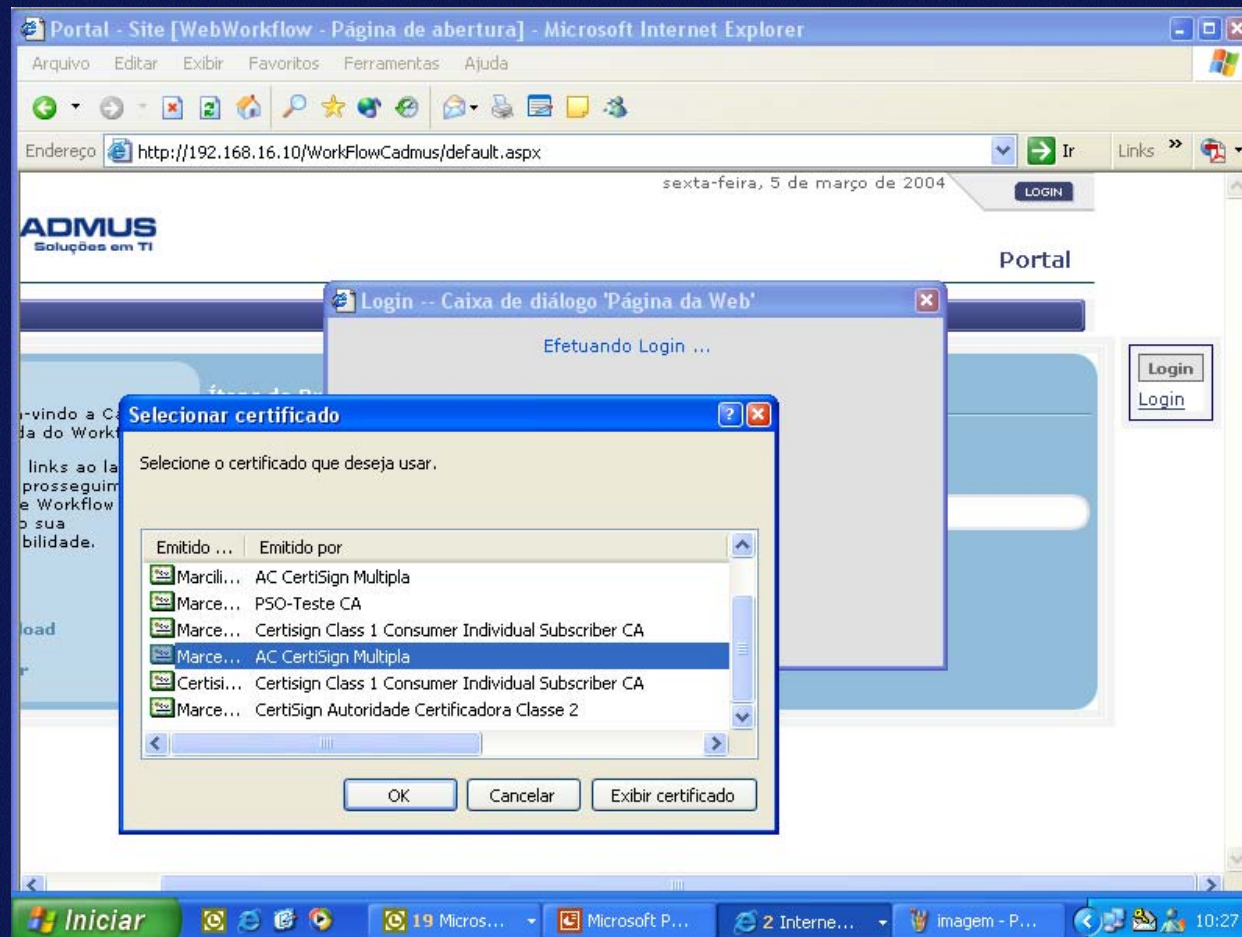
VeriSign® < Anterior Assinar Cancelar



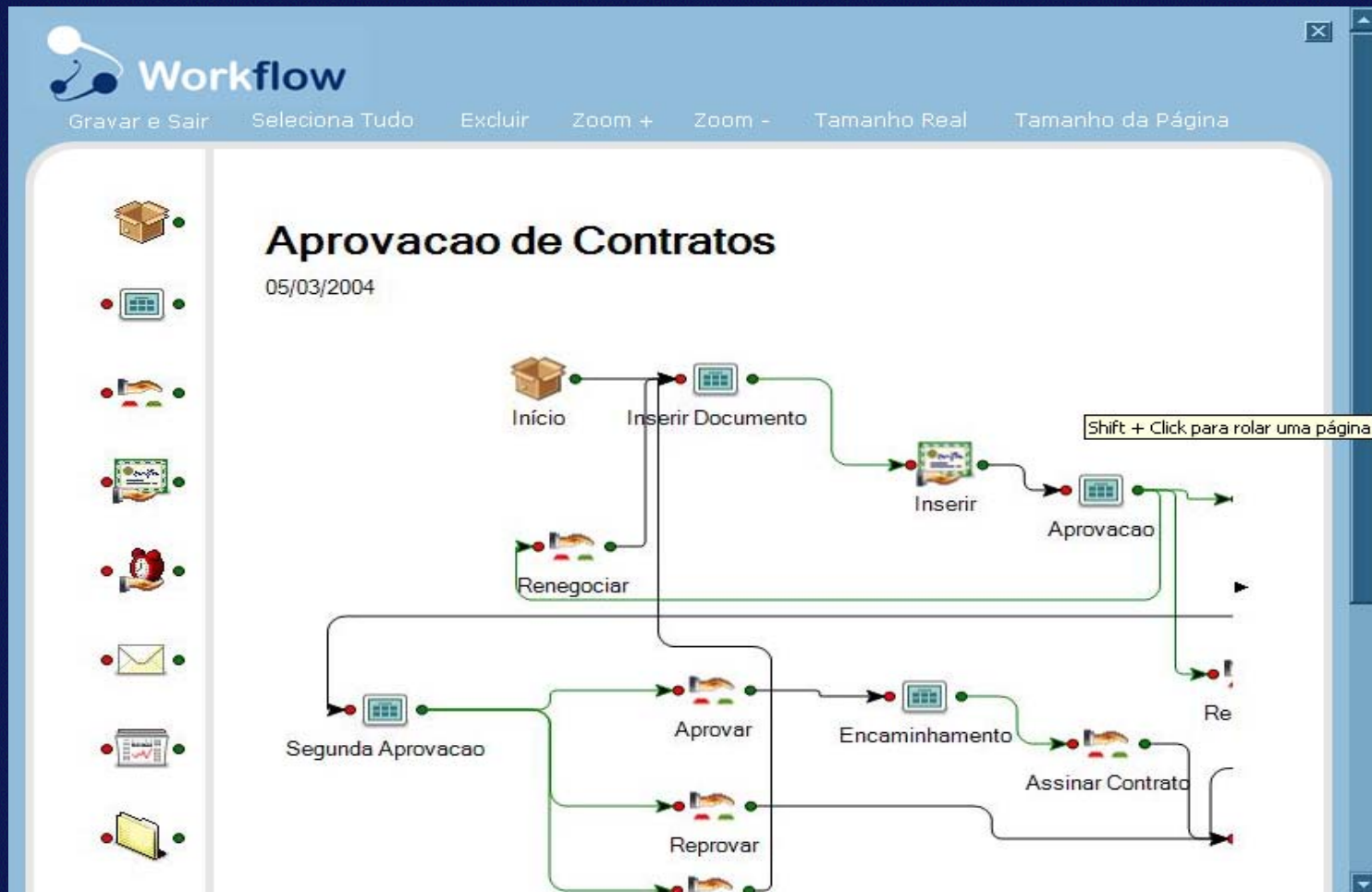
Diário Oficial

digitalsign Workflow – integração com Assinatura Digital de Documentos

- Autenticação do utilizador por CERTIFICADO DIGITAL



➤ Desenhando um fluxo




Caixa de entrada do utilizador


Processos

Marcelo Sponchiado,
seja bem-vindo a Caixa de Entrada do Workflow.

Utilize os links ao lado para dar prosseguimento a itens de Workflow que estão sob sua responsabilidade.

Legenda

 **Download**

 **Excluir**


Ítems de Processo

Processo

Todos

Prioridade

Todas

| Apelido | Nome do Item | Processo | Etapa | Prioridade | Situação | Delegado Para | Excl |
|-----------------------|--------------------------------|------------------------|------------------------|------------|---------------------|---------------|---|
| Contrato Privado | Processo 22535 | Solicitacao de compra | Solicitacao | Urgente | material solicitado | | |
| Novo Processo | Processo 22536 | Solicitacao de compra | Compras | Alta | material solicitado | | |
| Novo Processo jacques | Processo 22538 | Solicitacao de compra | Aprovacao da Diretoria | Alta | material solicitado | | |
| Novo Processo | Processo 22537 | Solicitacao de compra | Solicitacao | Normal | material solicitado | | |
| Novo Processo | Processo 22539 | Solicitacao de compra | Aprovacao da Diretoria | Normal | material solicitado | | |
| Contrato de Venda | Processo 22553 | Aprovacao de Contratos | Aprovacao | Normal | documento inserido | |  |

Anterior

Próximo

- Correio Electrónico

- Garante a confidencialidade da informação transmitida
- Equivalente à carta fechada (ainda mais seguro)
- Garante a autenticação e a integridade dos dados enviados
- Após aposta a assinatura, não pode negar que o fez (não repudiação)

- Intranet/Extranet

- Substituição do *login-password*
- Ideal para funcionários, clientes, fornecedores
- Maior credibilidade e segurança

- Sistema Financeiro

- Autenticação e validação do utilizador perante a Instituição
- Facilidade de utilização
- Legalmente vinculativo (assinatura digital)
- Economia de custos

- Serviços Públicos

- Utilização dos certificados emitidos por uma entidade central nos diversos serviços públicos
- Acesso web aos serviços
- Redução de pessoal

- Comércio electrónico
 - Possibilidade de utilização dos certificados emitidos por outras Instituições, como por exemplo, um Banco
 - Legalmente vinculativo, através da assinatura digital
 - Acrescentando bens/serviços à oferta, tirando partido da “partilha” de certificados
- ...

- **As organizações já executam processos críticos para a sua missão através da Internet, SEM SEGURANÇA**
- **A Assinatura Digital tem como desafio permitir a transição para o meio digital, sem precisar abdicar da Segurança.**
- **Assinatura Digital**
 - Trata-se de uma tecnologia estável e madura..
 - Possui todo o suporte legal necessário.

A assinatura digital já é realidade!

■ Álvaro Matos

• Director Técnico

- DigitalSign
- Web: www.digitalsign.pt

• Endereço:

- Largo Pe. Bernardino
Ribeiro Fernandes, 26
4810-737 Nespereira
Guimarães

• Contacto:

- Tel: 253560642
- Fax: 253560639
- email: amatos@digitalsign.pt

