INTRODUÇÃO A CRIPTOGRAFIA

Sérgio Roberto de Lima e Silva Filho

Consultor

Agipro Sistemas Computacionais e Consultoria Ltda.

AGENDA

INTERNET

- O que é a internet?
- Tipos de Transações.
- Problemas da Internet.
- Ameaças de Segurança na Internet.
- Requisitos de Segurança.

O QUE É A INTERNET?

Internet

– Rede de computadores de âmbito mundial, **descentralizada e de acesso público**, cujos principais serviços oferecidos são o correio eletrônico e a WEB. (Aurélio)

– Interligação de rede de computadores existentes.

– Protocolo TCP-IP

– Conjunto de tarefas e serviços:

- FTP (Arquivos);
- E-mail (Correio Eletrônico);
- www (WEB), etc...

World Wide Web - WWW

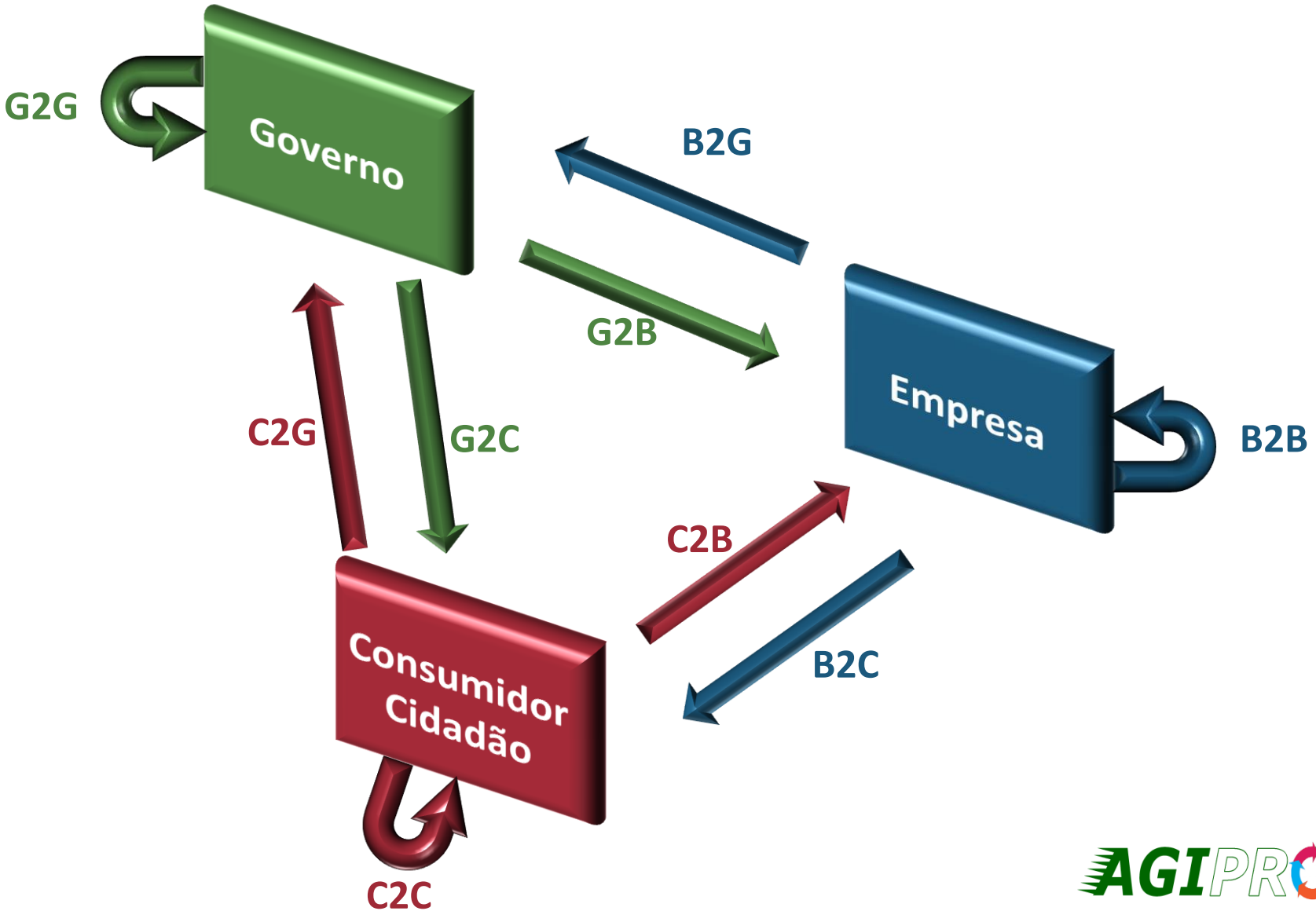
– Sistema de hipermídia disponível na internet, com documentos e outros objetos localizados em pontos diversos da rede e vinculados entre si. (Aurélio)

– Emaranhado de documentos, figuras, arquivos, vídeos, serviços, recursos, etc...

– Anonimato e desconfiança.

Internet – Nuvem

Transações realizadas na Internet



Problemas da Internet

Fontes de Problemas e Fragilidades

– A internet não foi concebida para ser segura.

– Inexperiência, desatenção e desconhecimento.

– Falta de políticas de Segurança.

– Direitos Autorais e Propriedade Intelectual.

– Identificação dos usuários e anonimato.

– Computação em “Nuvem”.

– Cibercrime.

Hackers apoiados pelo Irã atacam sites de energia dos EUA

Invasores se infiltraram nos sistemas de companhias de energia, diz jornal. Hackers iranianos passaram a ser mais preocupantes que chineses.

Da Agência EFE

6 comentários Tweetar 126 Recomendar 122

Hackers apoiados pelo Irã 'intensificaram sua campanha de ataques' contra empresas dos Estados Unidos se infiltrando nos sistemas de companhias de energia, informou nesta sexta-feira (24) o jornal "The Wall Street Journal".

24 de Maio de 2013 - 12h05

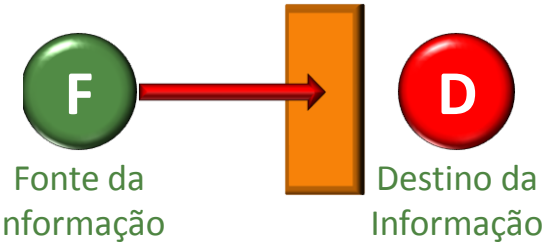
Anonimato

Fabricação

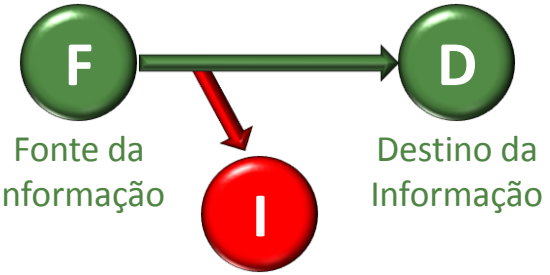
Ameaças de Segurança da Internet

Fluxo Normal da Informação

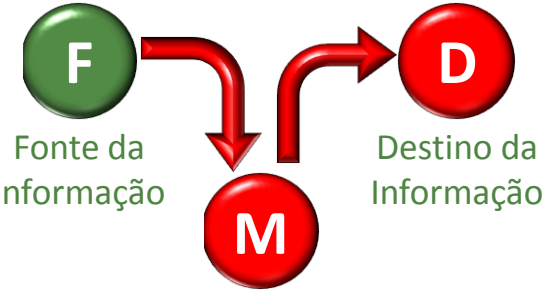
Interrupção



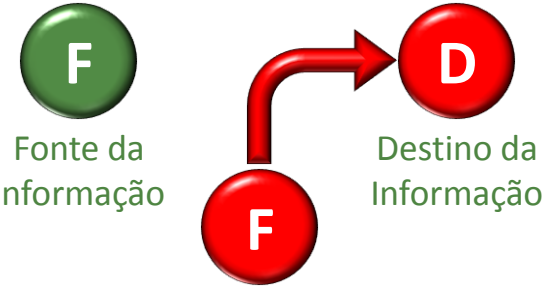
Interceptação



Modificação



Fabricação



Requisitos de Segurança

Sigilo	• Garantia de privacidade das informações. • Apenas os responsáveis tem acesso.
Integridade	• Garantia de que uma determinada informação não sofreu alterações.
Autenticidade	• Garantia da autoria da informação. • Garantia de origem.
Não Repúdio	• Impossibilidade de negar a autoria da informação.
Tempestividade	• Garantia da data/hora da informação. • Garantia da relação de precedência.

AGIPRO

CRIPTOGRAFIA SIMÉTRICA

- O que é a criptografia?
- Criptografia Simétrica.
- Técnicas Clássicas.
- Técnicas Modernas.
- Gerenciamento de chaves.
  - Problema na Troca de chaves – Ataque do homem do meio.
- Vantagens, Desvantagens e Conclusão.

AGIPRO

O QUE É CRIPTOGRAFIA?

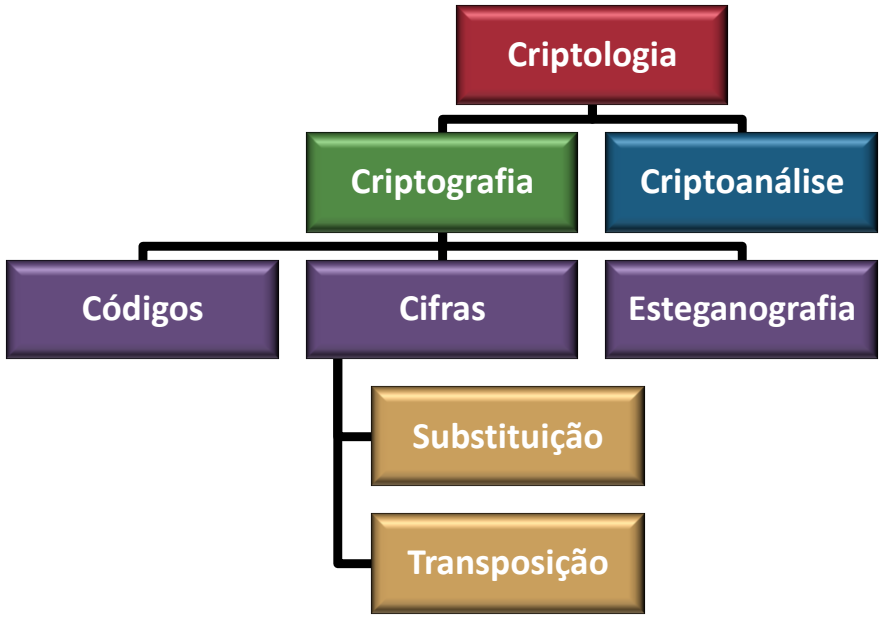
Criptografia

– Do Grego kryptós, "escondido", e gráphein, "escrita“.

– Escrever informações de forma escondida e que apenas o destinatário possa reconhecer.

– Técnicas Clássicas, Modernas e Quânticas.

Criptologia



Terminologias

– Texto Plano, original ou Claro: Este é um exemplo de texto plano

– Texto Cifrado: Ftuf f vn fzfnqmp ef ufzup qmbop

– Cifrar: Texto Plano → Texto Cifrado

– Decifrar: Texto Cifrado→ Texto Plano

– Chave: Informação usada para cifrar/decifrar

– Algoritmo de Criptografia: regras de transformação

Introdução

– A chave é conhecida pela fonte da mensagem e pelo destino.

– A chave normalmente é trocada através de um meio seguro.

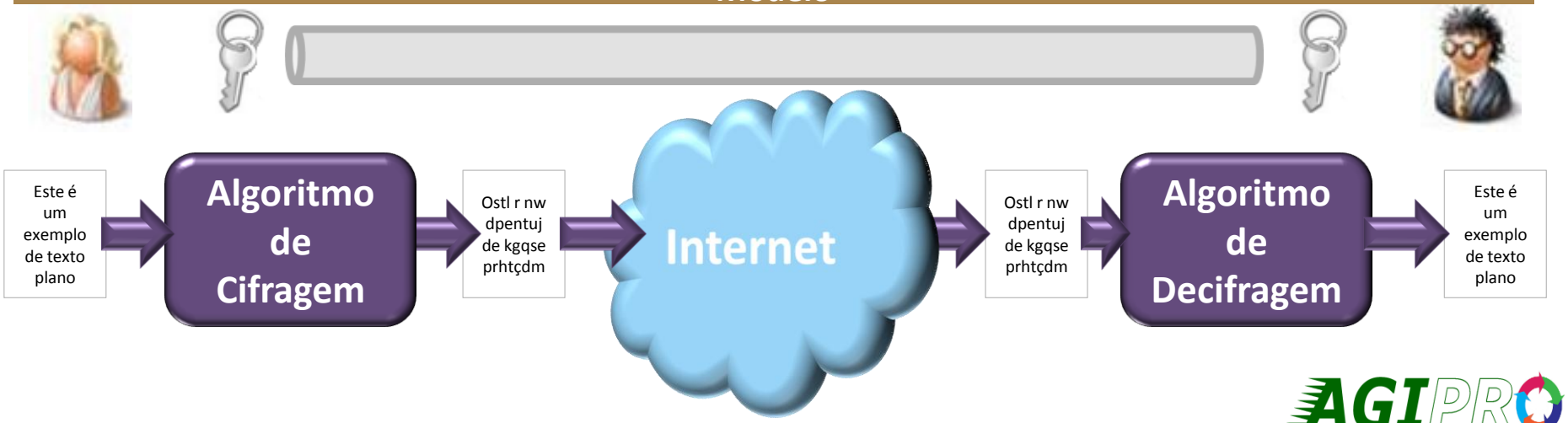
– Técnica com mais de 4.000 anos de existência (hieróglifos).

– busca da confidencialidade = sigilo.

– Classificações:

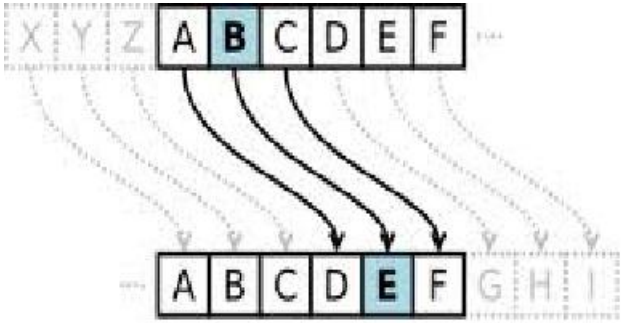
  – Criptografia Clássica.
  – Criptografia Moderna.
  – Criptografia Quântica.

Modelo



Bastão de Licurgo

Cifrador de César




```
Chave:     3
Plano:     Teste

cifrado:   Xhvxh
```

Cifra de Vegenère

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

```
Chave:     deceptivedeceptivedeceptive
Plano:     wearediscoveredsaveyourself

cifrado:   ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

One Time Password

– Senha para usar uma única vez.

– Executada operação ⊕ entre chave e texto plano.

Chave:	0	1	1	1	0	0	1	0	1	1	0
⊕											
Plano:	1	1	0	0	0	1	1	1	0	1	0
Cifrado:	1	0	1	1	0	1	0	1	1	0	0

AGIPRO

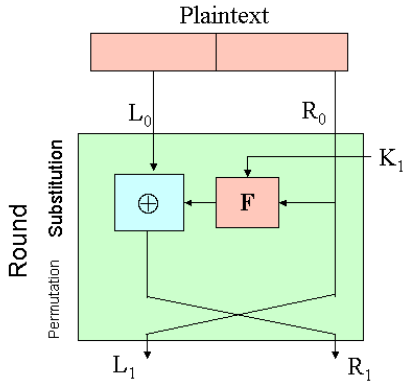
Alguns princípios de Kerckhoffs - 1883

– Comprometimento do algoritmo não deve comprometer a comunicação.

– Chave deve ser memorizável e facilmente alterada.

– O segredo deve estar na chave e não no algoritmo.

Estrutura de Feistel (IBM, 1973)



L_0 = left half of plaintext
R_0 = right half of plaintext

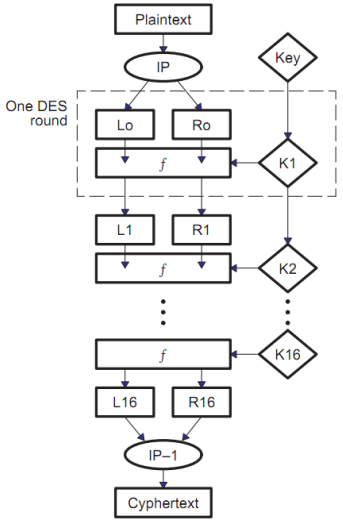
$L_i = R_{i-1}$
$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$

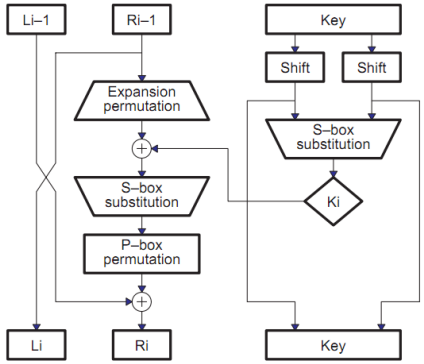
$C = R_n \| L_n$
n is number of rounds
(undo last permutation)

Características das Técnicas modernas

– Tamanho variável da chave.
– Algoritmo de geração de sub-chaves.
– Operações Mistas (Substituição e Transposição).
– Rotação dependente da chave.
– Rotação dependente dos dados.
– Função F variável.
– Comprimento do Bloco variável.
– Número variável de fases.
– Operação nas duas metades de dados em cada fase.

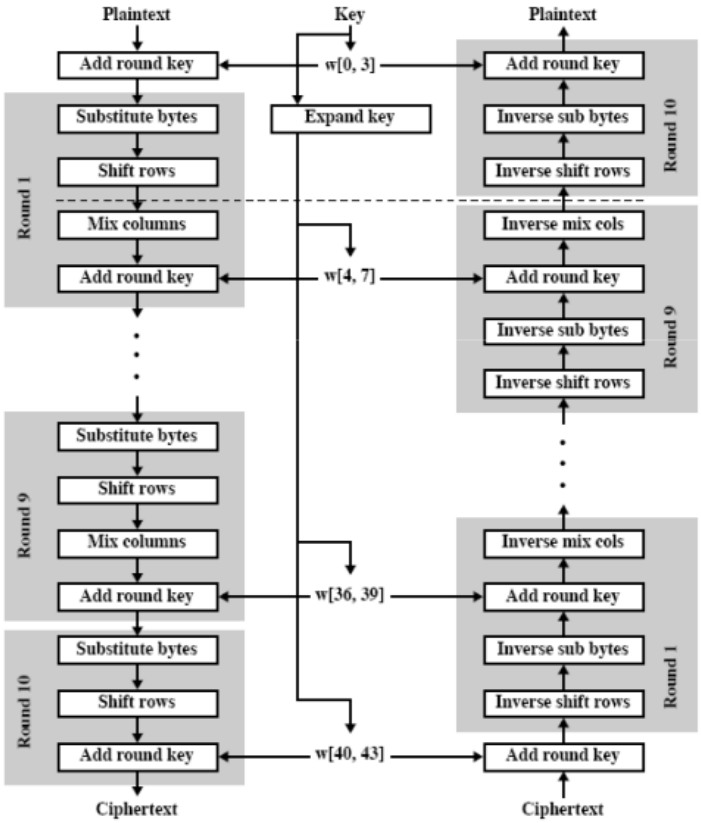
DES

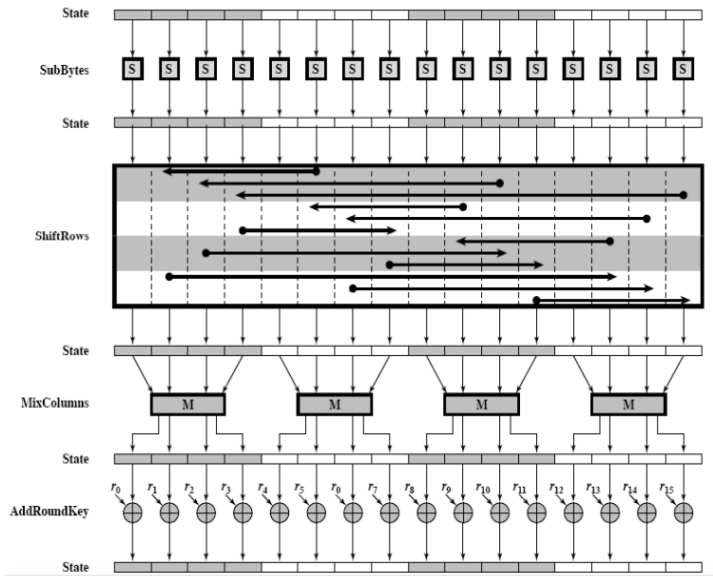


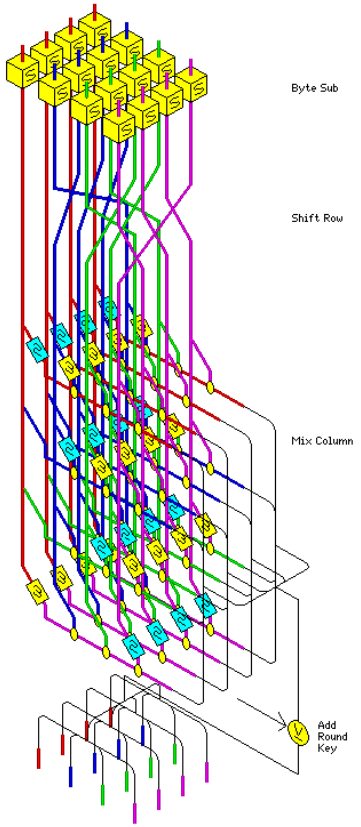


AES

Key size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext block size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of rounds	10	12	14
Round key size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded key size (words/bytes)	44/176	52/208	60/240



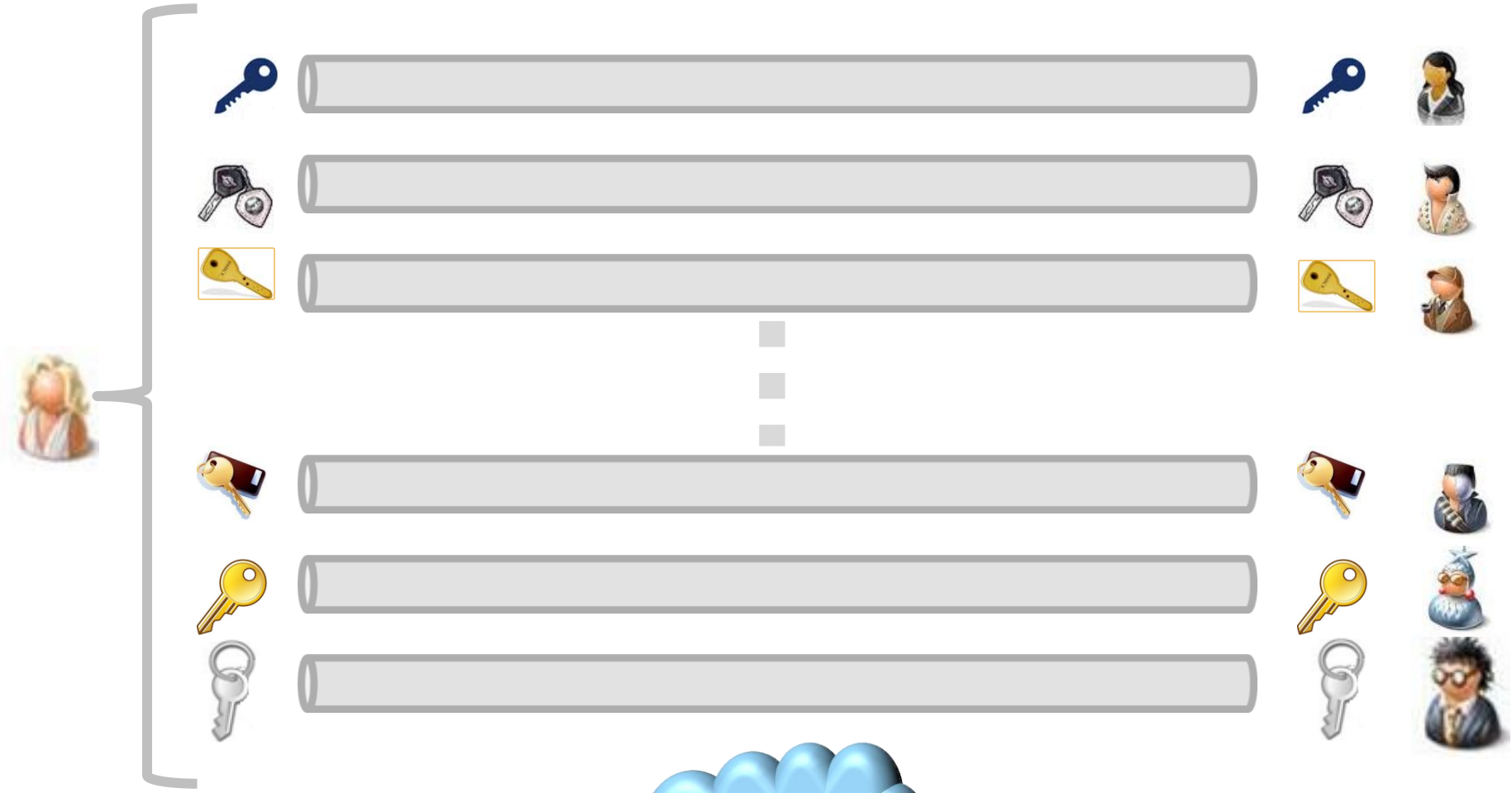




Outros Cifradores Simétricos

- 3DES.
- IDEA.
- Twofish e Blowfish.
- Serpent, AES, CAST5,
- RC4, RC5 e RC6.

Gerenciamento de Chaves



Este é um exemplo de texto plano

Algoritmo de Cifragem

Ostl r nw dpentuj de kgqse prhtçdm

Internet

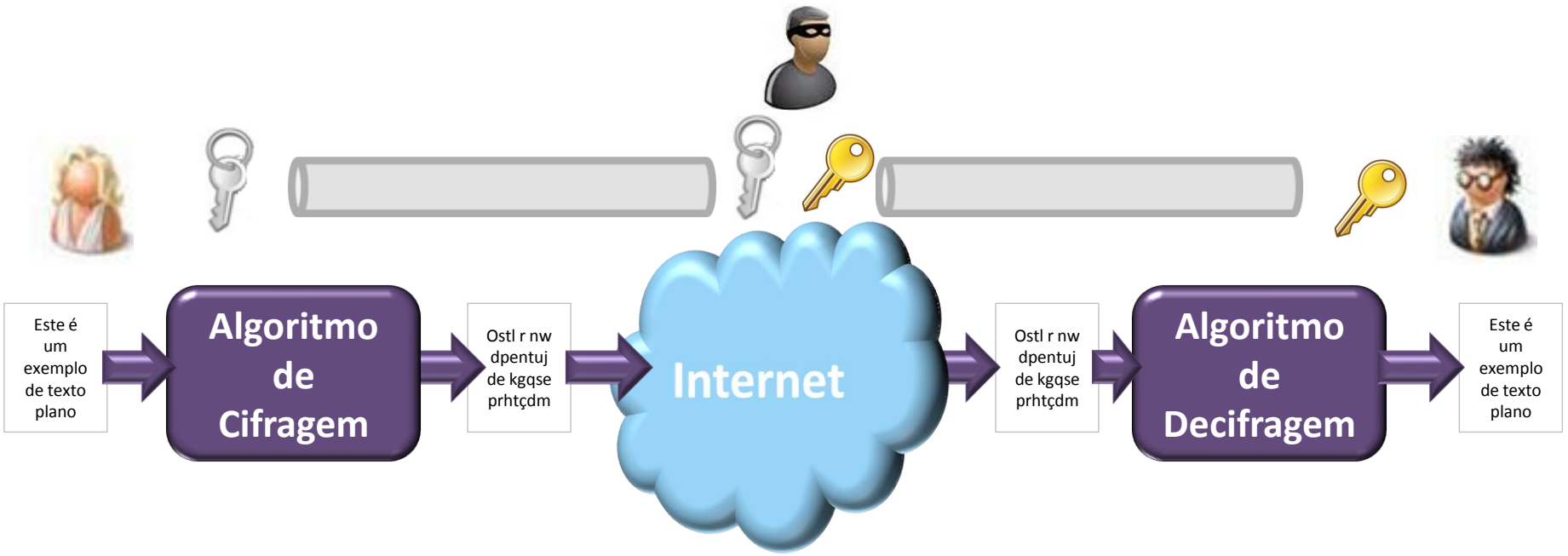
Ostl r nw dpentuj de kgqse prhtçdm

Algoritmo de Decifragem

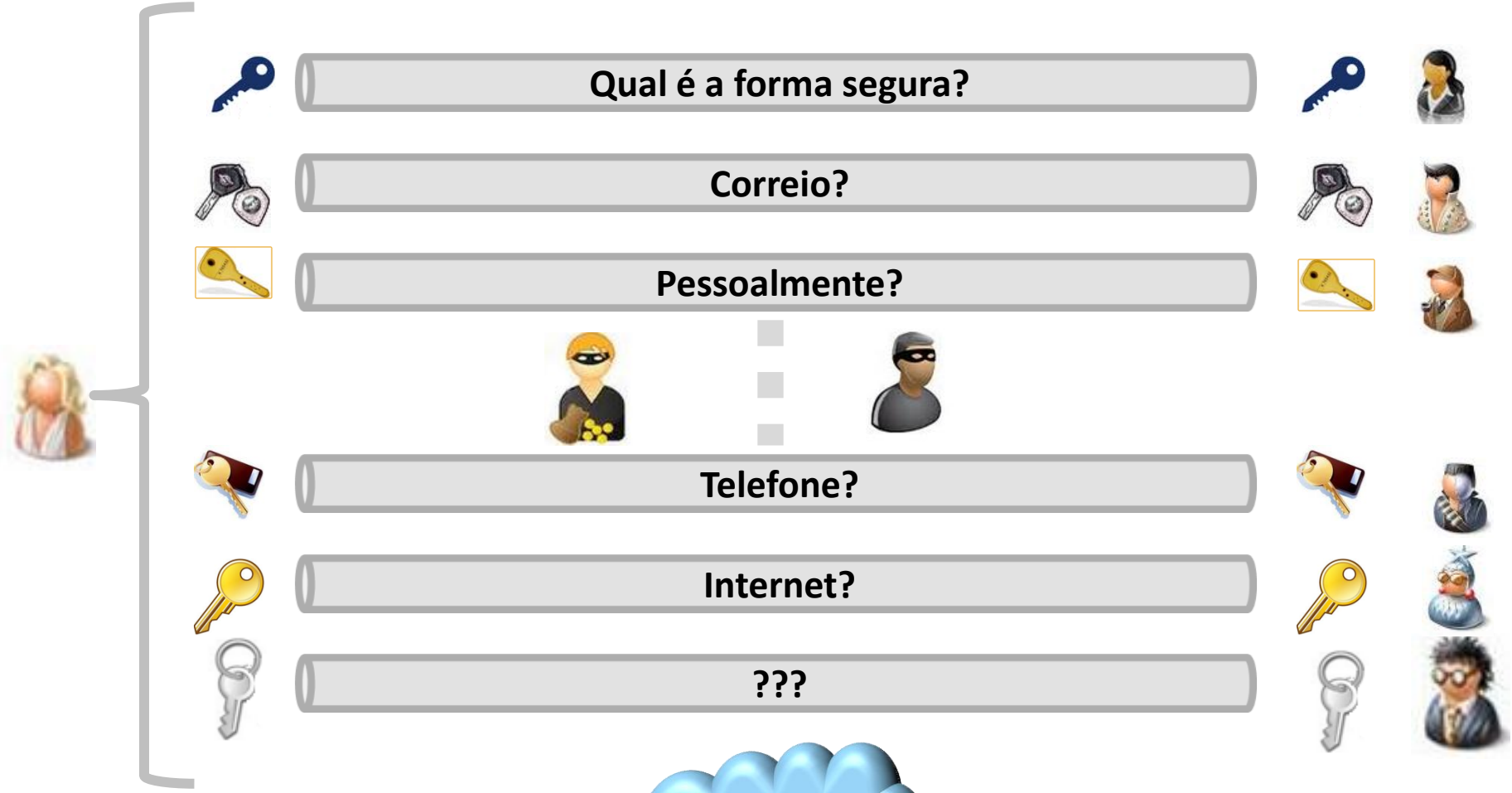
Este é um exemplo de texto plano

AGIPRO

Problema na Troca de Chaves – Ataque do Homem do Meio



Gerenciamento de Chaves



Vantagens, Desvantagens e Conclusão.

Vantagens

– Rápido.

– Seguro.

– Resolve o problema da confidencialidade.

– Permite estabelecer canal seguro na internet, para trocar informações críticas.

Desvantagens

– Dificuldade no gerenciamento de chaves.

– Dificuldade para trocar as chaves simétricas.

– A publicação da chave compromete a informação.

– A perda da chave impossibilita abrir a informação.

Conclusão

– Texto cifrado é do tamanho do texto plano.
– Utiliza transposição e substituições dependentes da chave.
– Extremamente rápido.
– Utilizado para garantir o sigilo de informações.
– Cifra tão fácil quanto decifra.

AGIPRO

FUNÇÕES HASH

- O que é a função Hash?
- Exemplos de algoritmos.

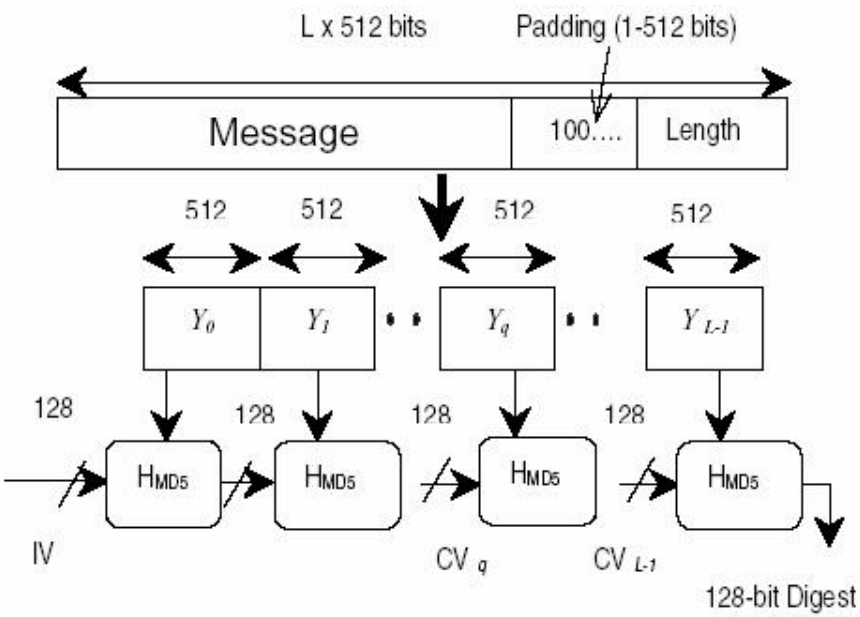
O QUE É FUNÇÃO HASH?

Definição

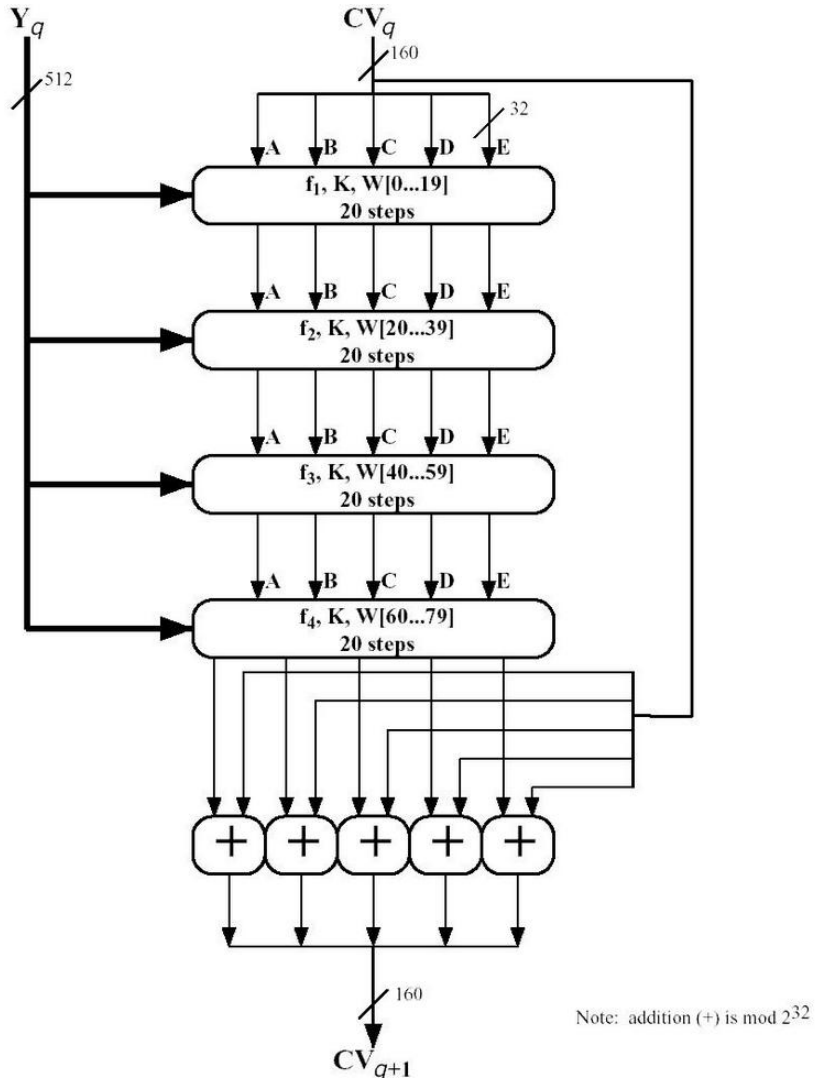
- A função HASH = resumo criptográfico = impressão digital.
- Converte uma grande quantidade de informação em uma **saída de tamanho fixo**
- Por definição, H(x) deve ser facilmente computado por hardware ou software.
- **One Way Property**:
  - Para um dado h, é **computacionalmente inviável** encontrar um x onde H(x) = h.
- **Weak Collision Resistence**:
  - Para um dado x, é **computacionalmente inviável** encontrar y ≠ x tal que H(x) = H(y).
- **Strong Collision Resistence**:
  - É **computacionalmente inviável** encontrar um par (x,y) tal que H(x) = H(y).
- Utiliza funções muito simples.
- Podem usar senha para gerar o hash.
- **Garante a integridade** de dados.

Exemplos de Algoritmos

MD5



SHA-1



Outros Algoritmos de HASH

– MD5 (Obsoleto) – mais ainda muito usado.

– RIPEMD-160.

– SHA 1, SHA 2 (SHA-256, SHA-384, SHA-512).

– Blake.

– HMAC.

CRIPTOGRAFIA ASSIMÉTRICA

- Criptografia Assimétrica.
  - RSA.
- Chave Pública x Chave Privada.
- Gerenciamento de chaves.
- Usos
  - Sigilo.
  - Assinatura Digital.
  - Sigilo e assinatura Digital.
- Criptografia Simétrica x Assimétrica.
  - Vantagens e Desvantagens.
- Conclusão.

AGIPRO

Introdução

– Também conhecida como criptografia de chaves públicas.

– Diffie e Hellman (1976): qualquer pessoa cifrar uma mensagem para um destino sem a necessidade de trocas de chaves secretas.

– Fundamento: Funções de caminho único (one-way) com trapdoor:

Função de Caminho Único			Função de Caminho Único c/ **trapdoor**		
$y = f(x)$	$\rightarrow$	fácil	$y = f_K(x)$	$\rightarrow$	fácil
$x = f^{-1}(y)$	$\rightarrow$	difícil	$x = f_K^{-1}(y)$	$\rightarrow$	fácil se K conhecido
			$x = f_K^{-1}(y)$	$\rightarrow$	difícil se K desconhecido

– Trabalha com pares de chaves: 1 Pública e 1 Privada (trapdoor).

– Impossibilidade de obter a chave privada tendo a chave pública e o algoritmo.

– RSA (1977): Baseado na dificuldade de fatoração de números primos grandes.

– Outro Algoritmos:

- ElGamal: baseado no problema do Log discreto.
- ElGamal sobre curvas elípticas.
- Etc..

RSA (Ron Rivest, Adi Shamir, Len Adleman)

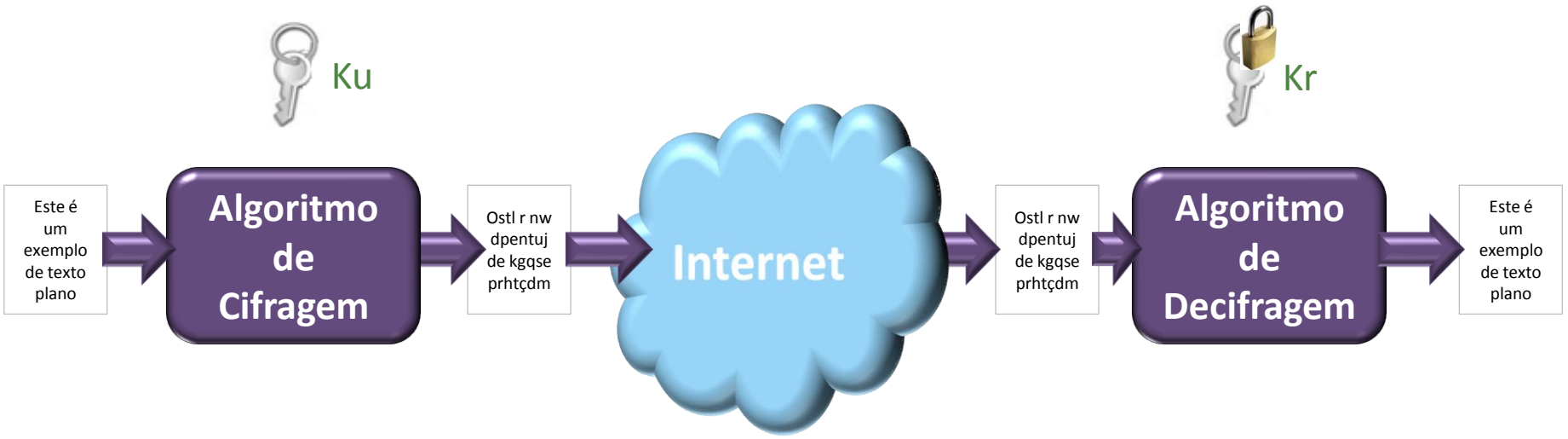
– Algoritmo mais utilizado atualmente:

$$\text{Texto Cifrado} = (\text{Texto Plano})^{e} \bmod n$$

$$\text{Texto Plano} = (\text{Texto Cifrado})^{d} \bmod n$$

$$Ku = \{e,n\} \qquad e = d^{-1} \pmod{\phi(n)}$$
$$Kr = \{d,n\}$$

Modelo



Chave Pública X Chave Privada

Chave Pública X Chave Privada

– Impossibilidade de se obter a chave privada a partir da chave pública.

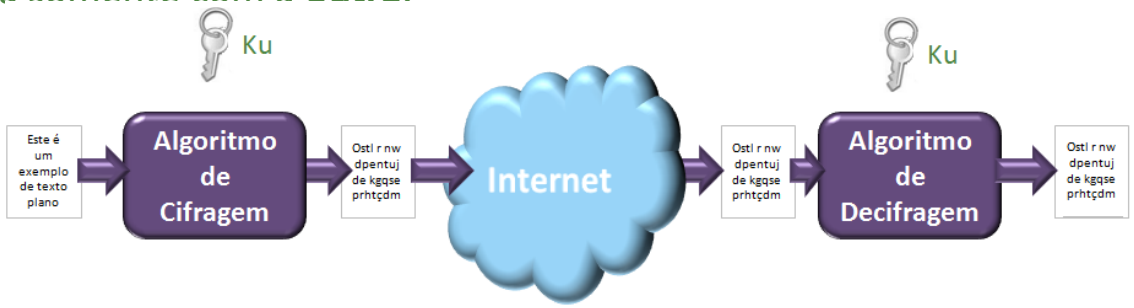
– Todas as entidades possuem as 2 chaves.

– Relação matemática:

- Cifra com 1 chave → Decifra somente com a **outra**.

– Permite agregar:

- Sigilo.
- Integridade.
- Autenticidade.
- Não Repúdio.



Chave Pública

– Todas as informações são públicas.

– Devem ser distribuídas livremente.

– Distribuída com o certificado digital.

Chave Privada

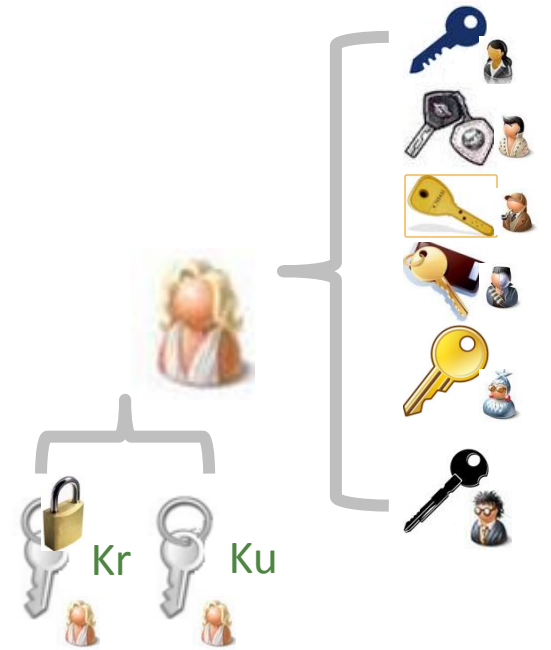
– Todas as informações são privadas.

– Devem ser mantidas em segredo.

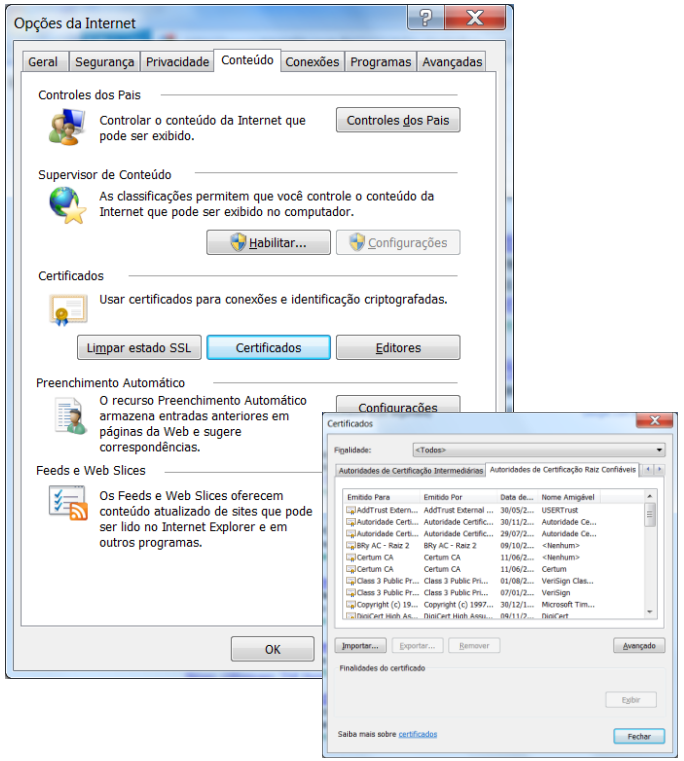
– Normalmente armazenadas em dispositivos de segurança:

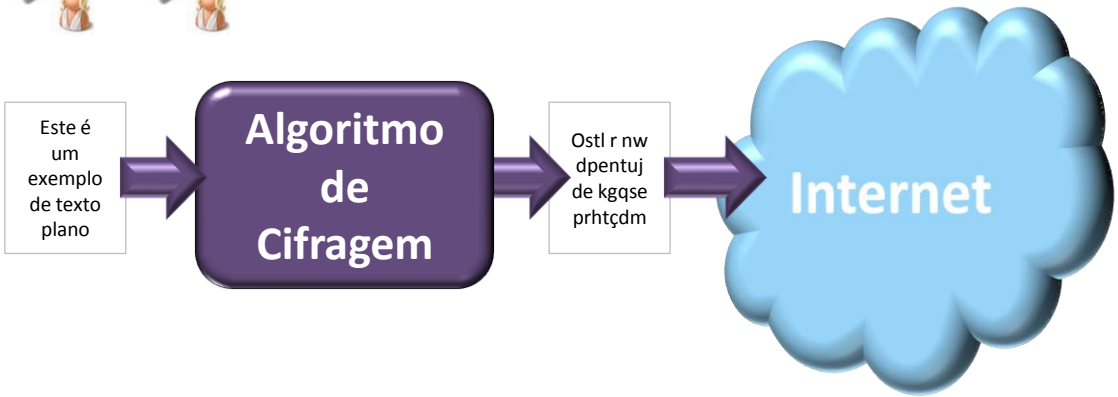
- Token.
- Smartcard.
- HSM.

Chaves usadas pelo usuário e exemplo de gerenciamento.



- Anuncio Público (PGP)
- Diretório Público
- Autoridade Certificadora
- Certificado Digital



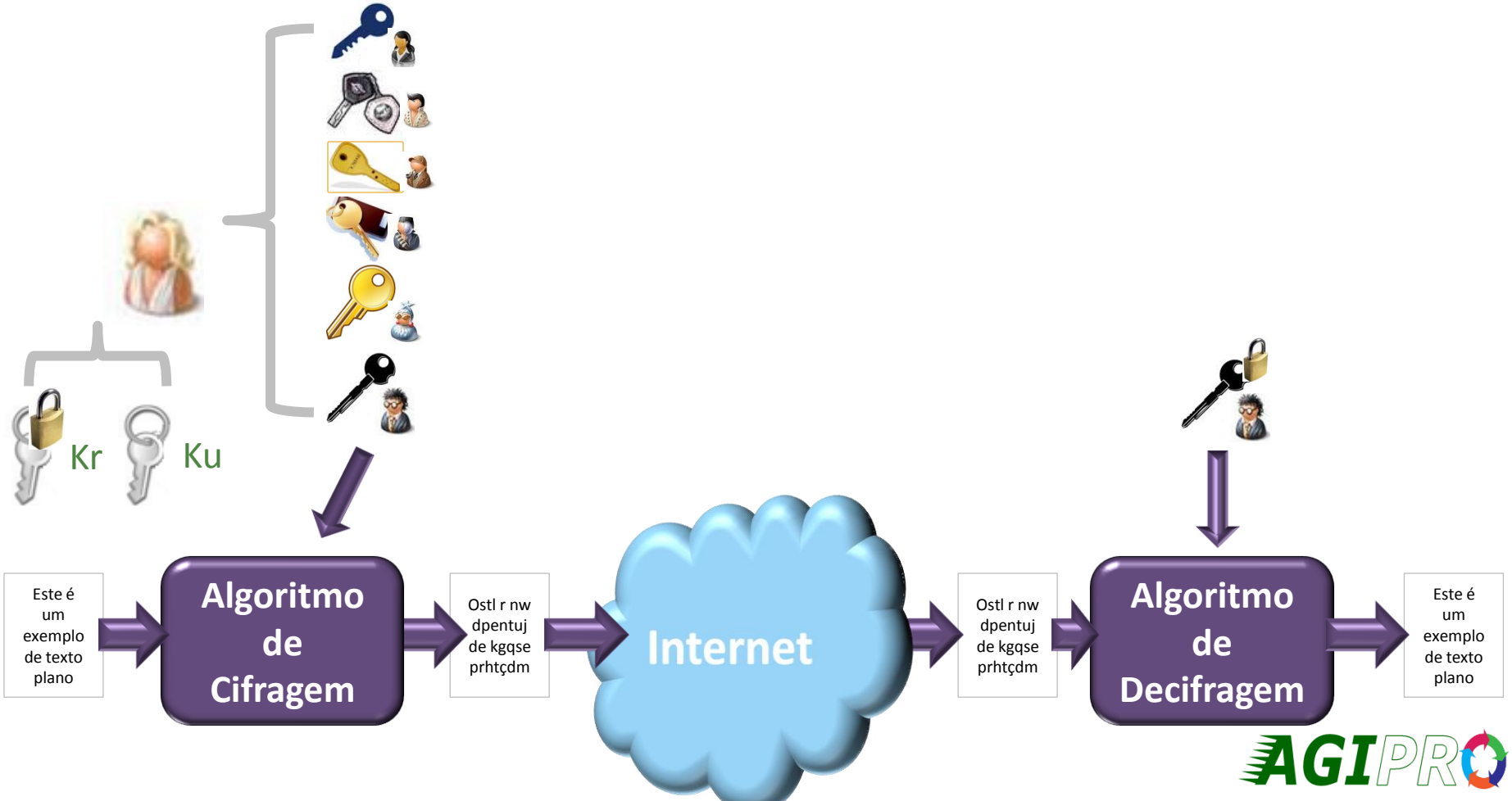


Usos

Sigilo

- Alice deseja enviar uma mensagem cifrada para bob.

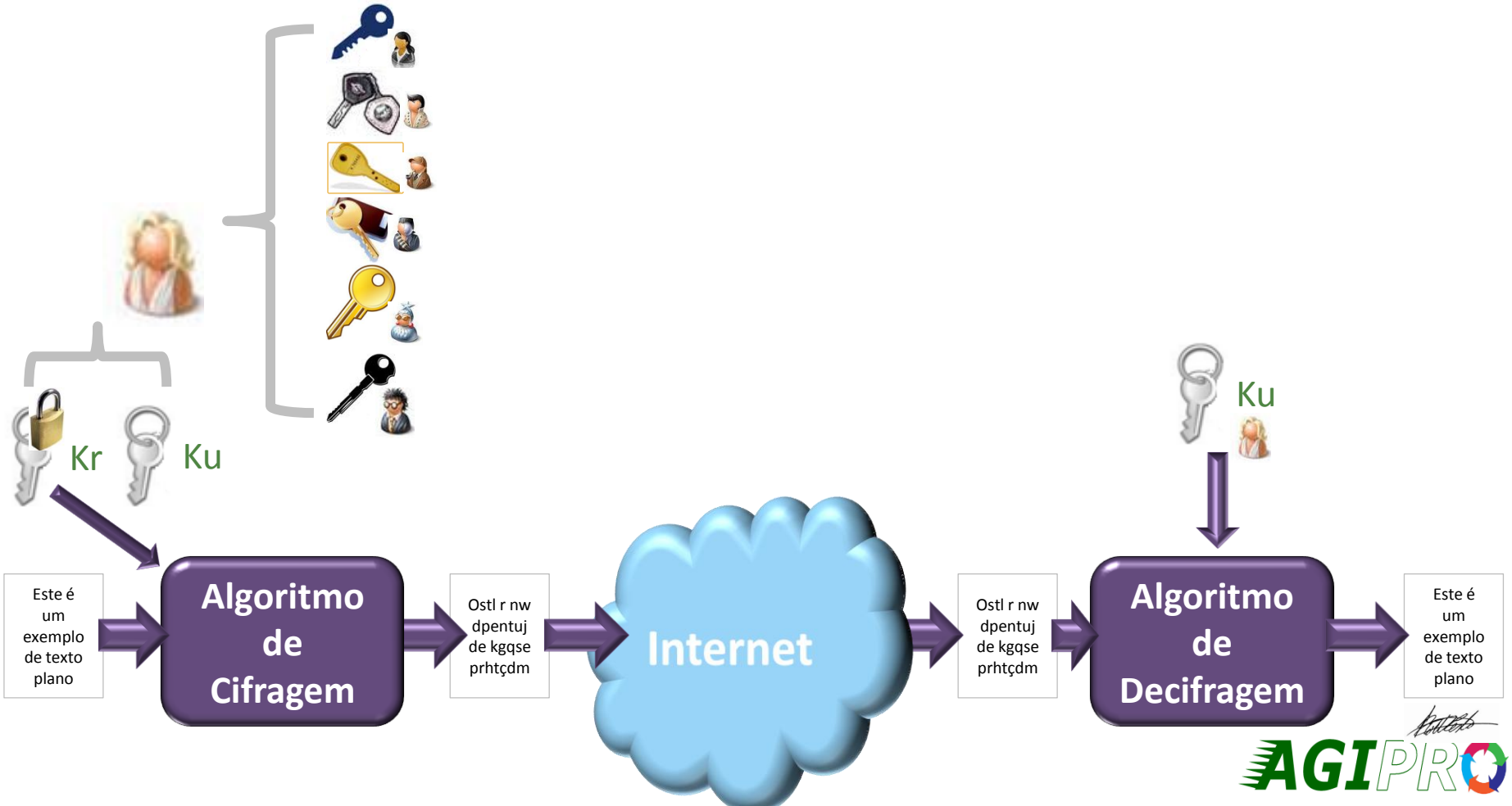
- Quais chaves deverão ser utilizadas para cifrar e decifrar a mensagem?



Assinatura Digital

- Alice deseja enviar uma mensagem assinada para bob.

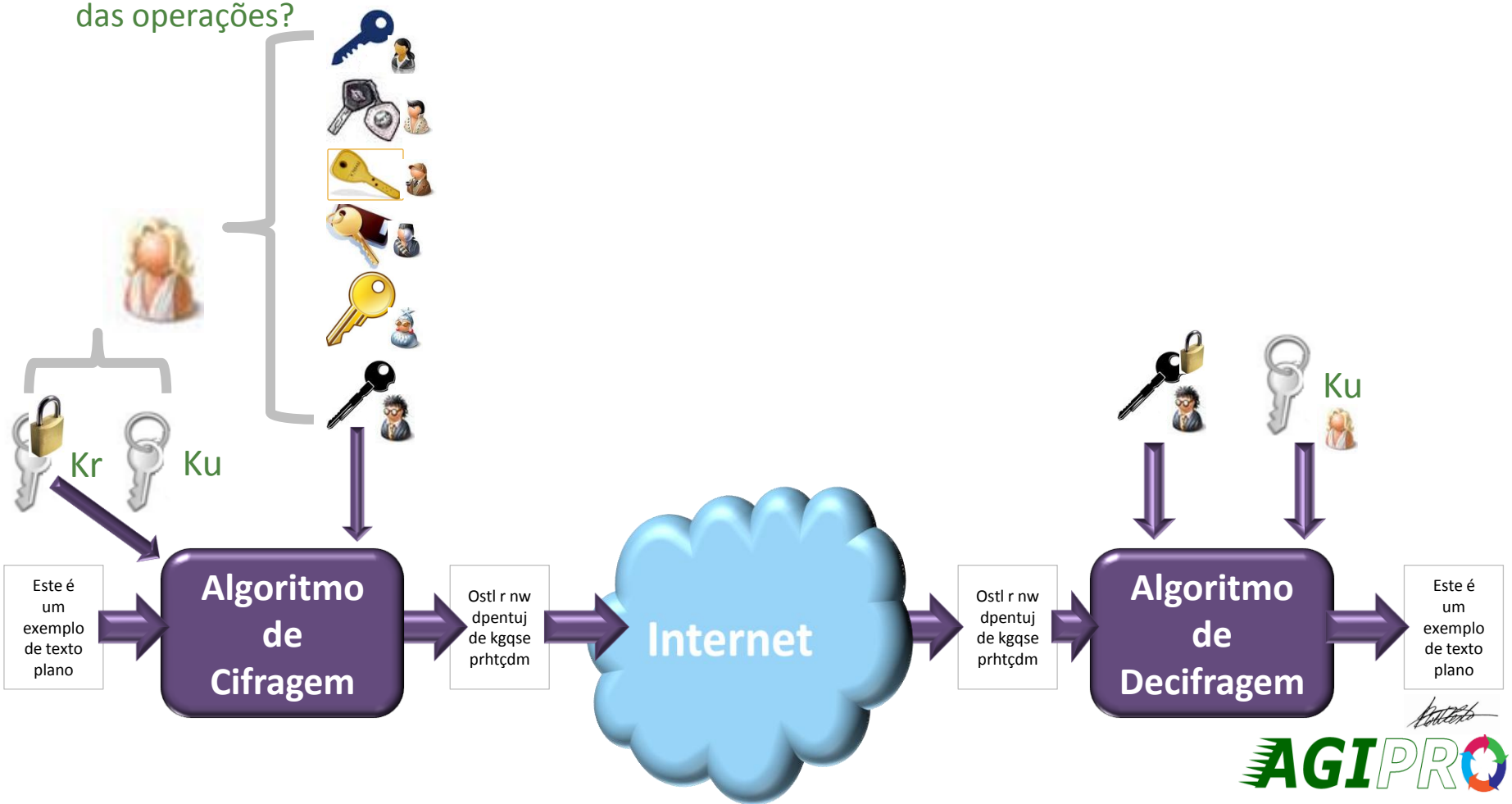
- Quais chaves deverão ser utilizadas para cifrar e decifrar a mensagem?



Sigilo e Assinatura Digital

- Alice deseja enviar uma mensagem sigilosa e assinada para bob.

- Quais chaves deverão ser utilizadas para cifrar e decifrar a mensagem? Qual deve ser a ordem das operações?



Criptografia Simétrica X Criptografia Assimétrica

Criptografia Simétrica

– A mesma chave é usada para cifrar e decifrar.

– O segredo esta na chave compartilhada.

– Chaves compartilhadas. Duplo risco de perda.

– Rápido.

– Problema no gerenciamento de chaves e na troca de chaves.

– Cifra bloco de tamanho ilimitado.

Criptografia Assimétrica

– Chaves distintas são usadas para cifrar e decifrar.

– O segredo está em apenas uma chave.

– Apenas uma chave pública compartilhada.

–Pode ser extremamente lento.

– Facilita o gerenciamento de chaves e a troca de chaves.

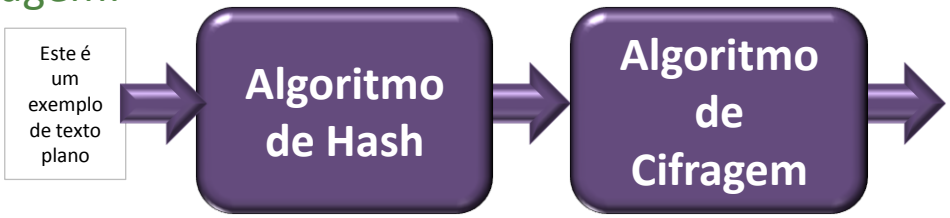
– O tamanho dos blocos pode ser limitado pelo algoritmo.

AGIPRO

Conclusão da Criptografia Assimétrica

– Usada para assinatura digital:

- Problema do tamanho da mensagem:
  - HASH.

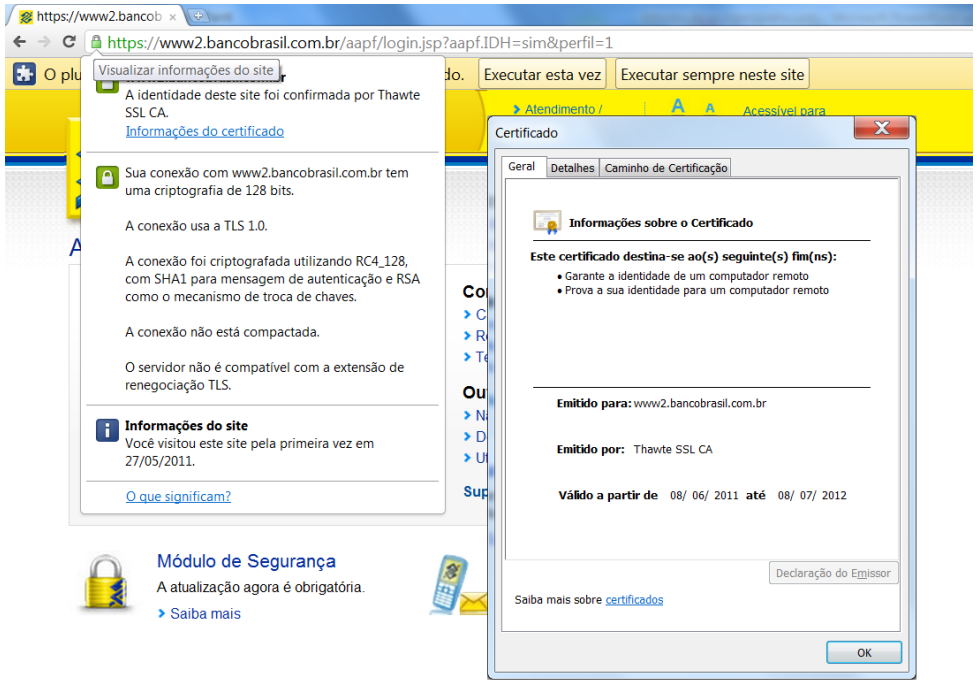


– Usada para sigilo de informações:

- Problema do tamanho da mensagem:
  - Senha simétrica.

– Usada para troca de chaves.

– SSL.



INFRAESTRUTURA DE CHAVES PÚBLICAS - ICP

- O certificado Digital.
  - Mundo Real x Mundo Digital
- O que é a infraestrutura de chaves públicas?
- A Autoridade Certificadora.
- A Autoridade de Registro.
- O Módulo Público.
- Passos para emissão de um certificado digital.
- Caminho de Certificação.
- Lista de Certificados Revogados.
- Tipos de certificados digitais.

Certificado Digital

– Certificado: Documento em que se certifica algo (Aurélio).

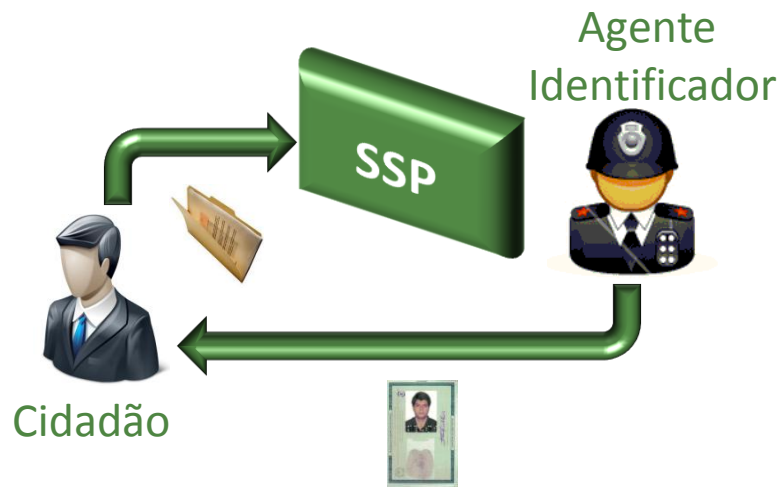
– Certificado Digital: Documento que certifica uma entidade no mundo Digital.

- Pessoas, sites, computadores, etc..

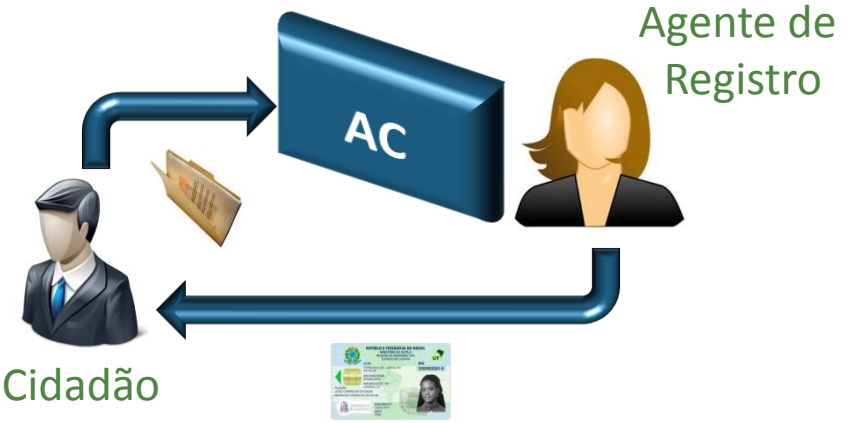
– Composição do certificado digital:

- Dados da entidade.
- Chave Pública.
- Campos de dados/Extensões.
- Assinatura da Autoridade emissora do certificado digital.

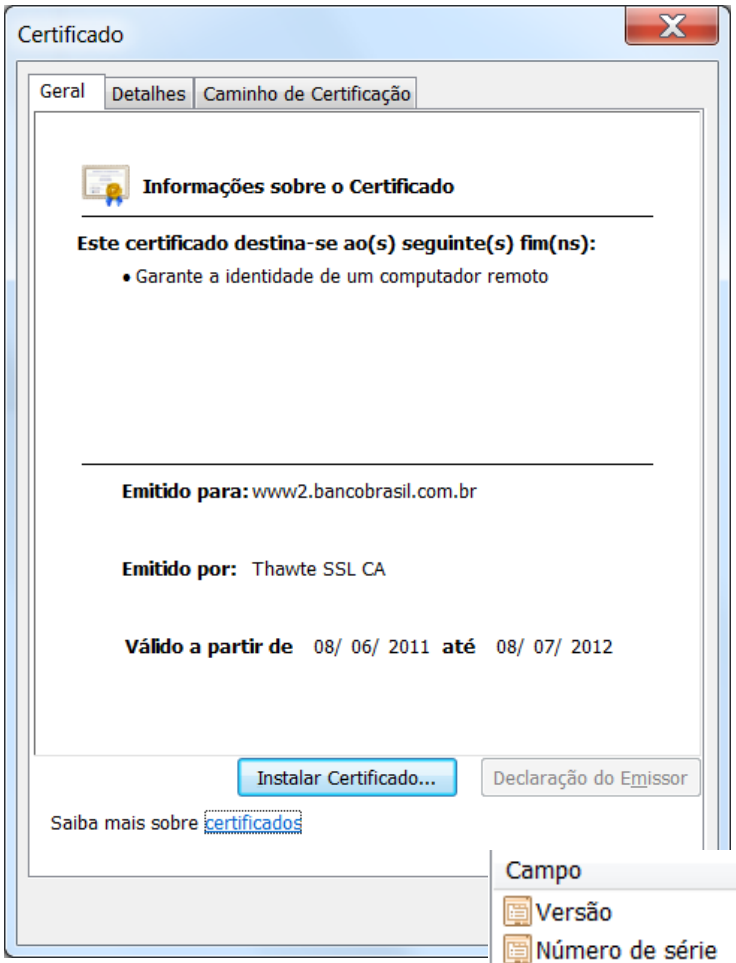
Mundo Real

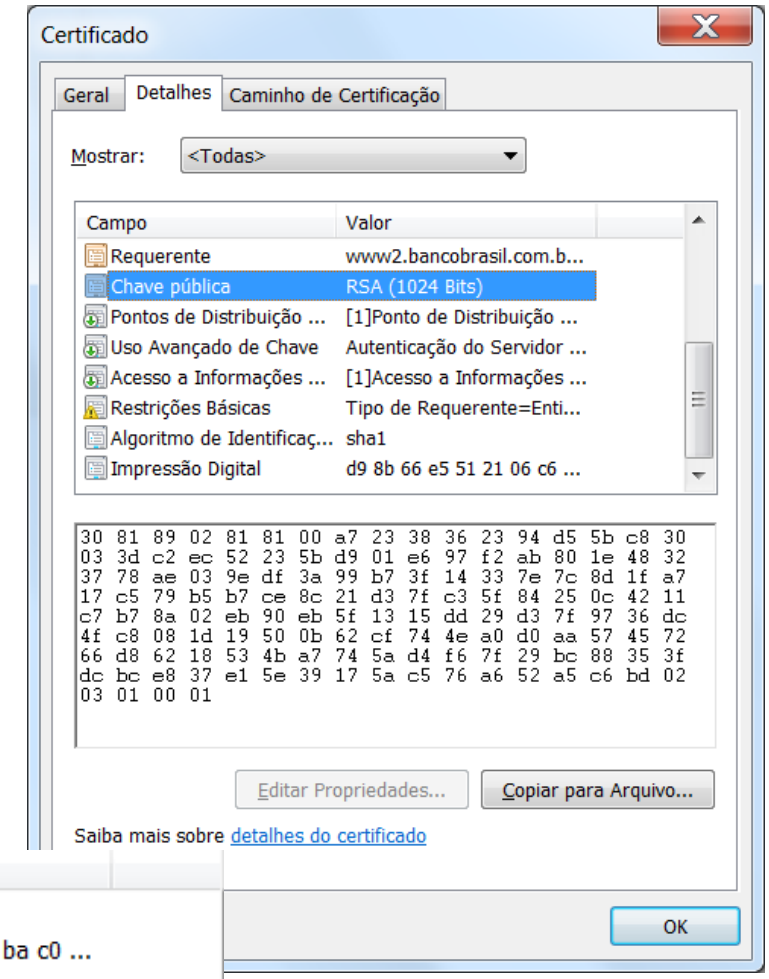


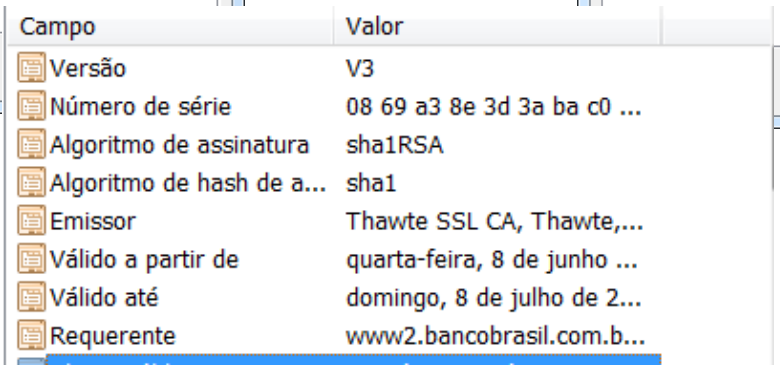
Mundo Digital ou Virtual



Informações e representação







Informações e representação – X509v3 (RFC 5280)

```
Certificate  ::=  SEQUENCE  {
     tbsCertificate       TBSCertificate,
     signatureAlgorithm   AlgorithmIdentifier,
     signatureValue       BIT STRING  }

TBSCertificate  ::=  SEQUENCE  {
     version         [0]  EXPLICIT Version DEFAULT v1,
     serialNumber         CertificateSerialNumber,
     signature            AlgorithmIdentifier,
     issuer               Name,
     validity             Validity,
     subject              Name,
     subjectPublicKeyInfo SubjectPublicKeyInfo,
     issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                          -- If present, version MUST be v2 or v3

     subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                          -- If present, version MUST be v2 or v3
     extensions      [3]  EXPLICIT Extensions OPTIONAL
                          -- If present, version MUST be v3
     }
```

Mídias de armazenamento

Smartcards e Leitoras

Tokens

HSMs

Computador

Infraestrutura de Chaves Públicas - ICP

– ICP é toda a infraestrutura necessária para emitir o certificado digital e controlar o seu ciclo de vida.

– Conjunto de hardware, software, políticas, procedimentos, pessoas e regulamentações.

– Princípio de confiança.

– Principais Módulos:

- Autoridade Certificadora.
- Autoridade de Registro.
- Módulo Público.

– **Autoridade**: Aquele que tem o direito ou o poder (Aurélio).

Infraestrutura de Chaves Públicas - ICP

Funcionamento Genérico (existem muitas variações)

1. Informa dados
2. Validação pelo Agente de Registro
3. Informações validadas encaminhadas para AC
4. Emissão do certificado Digital

Obs: As variações são decorrentes das regulamentações , políticas e procedimentos.

Autoridade Certificadora - AC

– Entidade responsável por:

- Emissão do certificado digital.
- Armazenamento e controle dos certificados digitais.
- Verificação da validação pela Autoridade de Registro.
- Revogação do certificado digital.
- Emissão da lista de certificados revogados.
- Armazenamento e controle da lista de certificados revogados.

– É o ambiente que exige maior segurança:

- Comprometimento → Invalida toda a ICP.
- Emite documentos com valor reconhecido.

– Tem que ser confiável.

– Segurança variável de acordo com políticas, regulamentações e procedimentos.

Autoridade de Registro - AR

– Entidade responsável por:

- Validação da validade dos dados do solicitante.
  - Presencial, ou
  - Remota
- Coleta de assinatura do termo de adesão.
- Assinatura dos dados para garantir validade dos mesmos para a AC
- Armazenamento e controle das documentações (dossiê da entidade solicitante).

– Ambiente:

- Comprometimento → Invalida apenas os certificados por ela validados.
- Emite validações de informações para a AC.

– Tem que ser confiável.

– Segurança variável de acordo com políticas, regulamentações e procedimentos.

Módulo Público

– Não é uma entidade. Apenas um sistema de coleta de dados.

– Pode estar vinculado diretamente ao sistema da AR.

– Coleta das informações do certificado.

– Escolha do tipo de certificado.

– Geração do par de chaves.

– Normalmente onde é realizado o pagamento.

– Ambiente:

- Comprometimento → Não impacta na emissão de certificados digitais.

– Segurança variável de acordo com políticas, regulamentações e procedimentos.

Passos para emissão do Certificado Digital

– Informação dos dados para emissão do certificado digital. (onde ocorre: MP ou AR)

– Geração do par de chaves. (onde ocorre: MP ou AR).

- Chave privada fica apenas com o solicitante.
- Gera requisição:
  - Chave pública + dados: assinada com chave privada (comprovar posse da Chave Privada).

– Validação dos dados pelo Agente de Registro(onde ocorre: AR).

- Presencial (entidade precisa comparecer a AR) ou Remota.
- Apresentação ou envio dos documentos, conforme política.
- Assinatura de termo de adesão, conforme política.
- Validação dos dados pelo Agente AR.
- Assinatura dos dados para envio para a AC.

– Recepção dos dados assinados pela AR (onde ocorre: AC).

– Validação da assinatura da validação do agente AR (onde ocorre: AC).

– Validação da requisição do certificado digital. (onde ocorre: AC).

– Emissão do Certificado Digital(Assinado pela AC) e publicação do mesmo (onde ocorre: AC).

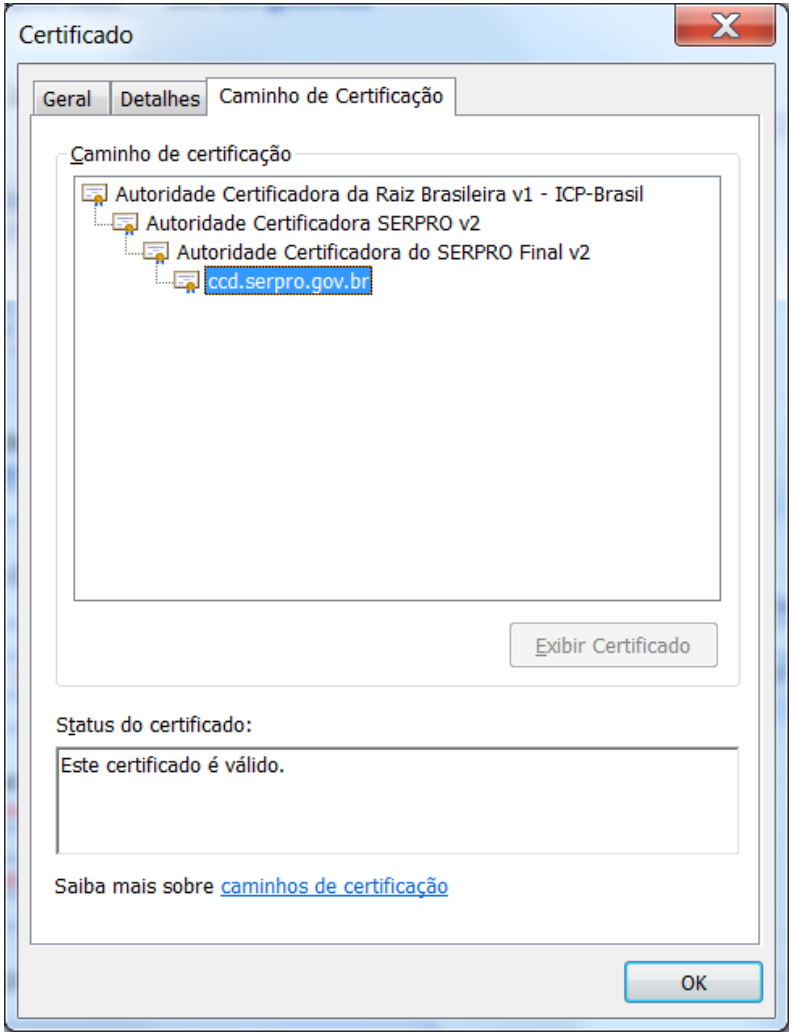
– Envio do certificado digital para AR ou MP.

– Instalação do certificado digital (onde ocorre: MP ou AR).

Caminho de Certificação

– É a hierarquia de emissão de certificados.

– Possibilita montar a cadeia de confiança.



Lista de Certificados Revogados - LCR

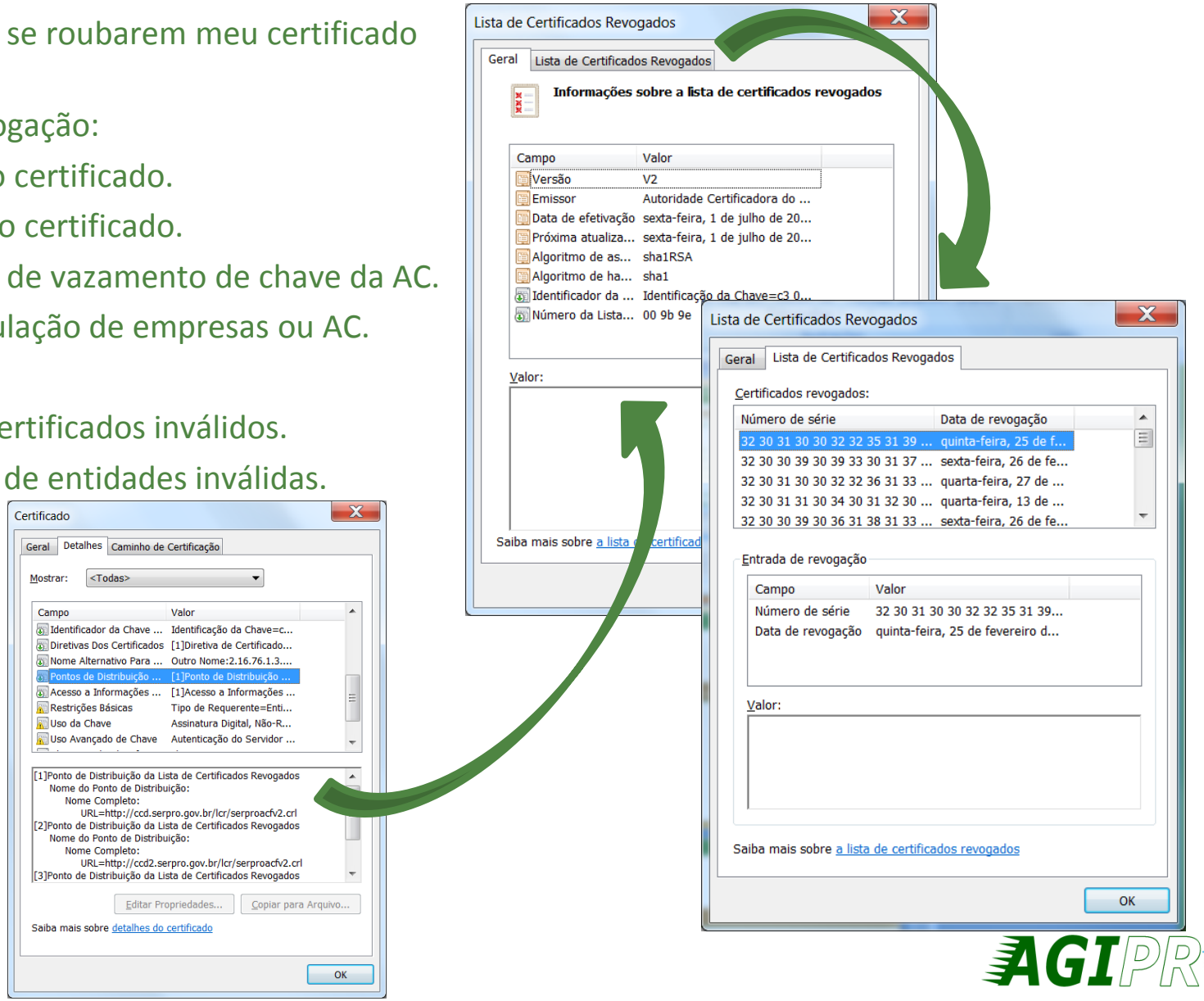
– O que acontece se roubarem meu certificado digital?

– Motivos de revogação:

- Perda do certificado.
- Roubo do certificado.
- Suspeita de vazamento de chave da AC.
- Desvinculação de empresas ou AC.
- Etc...

– É uma lista de certificados inválidos.

– Não é uma lista de entidades inválidas.



Lista de Certificados Revogados – LCR (RFC 5280)

```
CertificateList  ::=  SEQUENCE  {
     tbsCertList          TBSCertList,
     signatureAlgorithm   AlgorithmIdentifier,
     signatureValue       BIT STRING  }

TBSCertList  ::=  SEQUENCE  {
     version                 Version OPTIONAL,
                                  -- if present, MUST be v2
     signature               AlgorithmIdentifier,
     issuer                  Name,
     thisUpdate              Time,
     nextUpdate              Time OPTIONAL,
     revokedCertificates     SEQUENCE OF SEQUENCE  {
          userCertificate         CertificateSerialNumber,
          revocationDate          Time,
          crlEntryExtensions      Extensions OPTIONAL
                                   -- if present, version MUST be v2
                                }  OPTIONAL,
     crlExtensions           [0]  EXPLICIT Extensions OPTIONAL
                                   -- if present, version MUST be v2
                                }
```

```
CRLReason ::= ENUMERATED {
     unspecified             (0),
     keyCompromise           (1),
     cACompromise            (2),
     affiliationChanged      (3),
     superseded              (4),
     cessationOfOperation    (5),
     certificateHold         (6),
          -- value 7 is not used
     removeFromCRL           (8),
     privilegeWithdrawn      (9),
     aACompromise           (10) }
```

Tipos de Certificados Digitais

Tipos de Certificados

Usos da Chave

- Assinatura Digital
- Não Repúdio
- Codificação de Chaves
- Codificação de Dados
- Troca de Chaves
- Verificação de assinatura de Certificados Digitais
- Assinatura de LCR
- Somente Cifragem
- Somente Decifragem

Tipos de Certificados

- Autenticação de Cliente
- Autenticação de Servidor
- Assinatura de código
- Proteção de E-mail
- Carimbo do Tempo
- Assinatura de OCSP
- Assinatura Digital
- Sigilo

AGIPRO

LEGISLAÇÃO ATUAL

- Lei Modelo Uncitral – Comércio Eletrônico
- DIRECTIVA 1999/93/CE DO PARLAMENTO EUROPEU E DO CONSELHO
- Lei Modelo Uncitral – Assinatura Eletrônica
- Outros Países
- Mercosul
- Prova
- O Documento e o Documento Eletrônico
- Requisitos para validade jurídica dos documentos
  - Lei Brasileira
    - MP 2200-2.
    - Lei 11.419.
    - Lei 11.280.
- Outras leis Nacionais

Lei modelo da Uncitral sobre o comércio eletrônico (16 de Dezembro de 1996)

– **art 10:** Conservação das mensagens de dados

1) Quando a Lei requeira que certos documentos, registros ou informações sejam conservados, este requisito considerar-se-á preenchido mediante a conservação de mensagens eletrônicas, sempre que as seguintes condições sejam satisfeitas:

a) Que a informação que contenham seja acessível para **consulta posterior**;

b) Que as mensagens eletrônicas sejam **conservadas no formato no qual tenham sido geradas**, enviadas ou recebidas, ou num formato que se possa demonstrar que **representa exatamente as informações geradas**, enviadas ou recebidas;

c) Que se conserve, caso exista, **toda informação que permita determinar a origem e o destino das mensagens e a data e a hora quando foram enviadas ou recebidas**.

– **art 11:** Salvo disposição em contrário das partes, na formação de um **contrato**, a oferta e sua aceitação podem ser expressas por mensagens eletrônicas. **Não se negará validade ou eficácia** a um contrato pela simples razão de **que se utilizaram mensagens eletrônicas** para a sua formação.

– **art 12:** Nas relações entre o remetente e o destinatário de uma mensagem eletrônica, não se negará validade ou eficácia a uma declaração de vontade ou outra declaração pela simples razão de que a declaração tenha sido feita por uma mensagem eletrônica.

– **art 13, 14 e 15:** Comprovações do remetente e do destinatário e regras de envio e recebimento.

DIRECTIVA 1999/93/CE DO PARLAMENTO EUROPEU E DO CONSELHO (13 de Dezembro de 1999)

– relativa a um quadro legal comunitário para as assinaturas eletrônicas.

– considerando:

- definição de um quadro europeu para as assinaturas digitais e a cifragem
- proposta de diretiva do Parlamento Europeu e do Conselho relativa às assinaturas digitais
- Regras divergentes para reconhecimento legal nos estados-membros → quadro comunitário claro
- Promover a interoperabilidade dos produtos associados às assinaturas eletrônicas
- Não limitar a definição na emissão de certificados → registro, aposição de datas, repertórios, etc..
- os serviços de certificação: prestados por entidade pública, pessoa singular ou coletiva, quando estabelecida nos termos da legislação nacional;
- Contribui para a utilização e o reconhecimento legal das assinaturas eletrônicas na Comunidade
- as assinaturas eletrônicas → produzir efeitos legais e ser admitidas como meios de prova em processos judiciais perante as jurisdições dos Estados-Membros
- As assinaturas eletrônicas: utilizadas no sector público no âmbito das administrações nacionais e comunitárias e nas comunicações entre essas administrações, assim como com os cidadãos e os operadores econômicos, por exemplo em contratos públicos, em matéria de sistemas de fiscalidade, de segurança social, de saúde e judiciário
- aceitação generalizada dos métodos de reconhecimento das assinaturas eletrônicas
- domínios legais em que podem ser utilizados documentos eletrônicos e assinaturas eletrônicas é regida pelas legislações nacionais.

AGIPRO

DIRECTIVA 1999/93/CE DO PARLAMENTO EUROPEU E DO CONSELHO

Âmbito de aplicação e definições

– facilitar a utilização das assinaturas eletrônicas e contribuir para o seu reconhecimento legal

– Institui um quadro legal comunitário para assinaturas eletrônicas e para serviços de certificação

–Não cobre aspectos relacionados com a celebração e a validade de contratos nem afeta as normas e as restrições constantes da legislação, nacional ou comunitária, que regem a utilização de documentos.

– **Assinatura Eletrônica:** os dados sob forma eletrônicas, ligados ou logicamente associados a outros dados eletrônicos , e que sejam utilizados como método de autenticação

– **Assinatura Eletrônica Avançada:** uma assinatura eletrônica que obedeça aos seguintes requisitos:

a) Estar associada inequivocamente ao signatário
b) Permitir identificar o signatário;
c) Ser criada com meios que o signatário pode manter sob seu controlo exclusivo; e
d) Estar ligada aos dados a que diz respeito, de tal modo que qualquer alteração subseqüente dos dados seja detectável.

DIRECTIVA 1999/93/CE DO PARLAMENTO EUROPEU E DO CONSELHO

Âmbito de aplicação e definições

– **Certificado:** um atestado eletrônico que liga os dados de verificação de assinaturas a uma pessoa e confirma a identidade dessa pessoa

– **Certificado qualificado:** um certificado que obedece aos requisitos abaixo e é fornecido por um prestador de serviços de certificação

a) Uma indicação de que o certificado é emitido como certificado qualificado.
b) A identificação do prestador de serviços de certificação e o país em que está estabelecido
c) O nome do signatário ou um pseudônimo, que deve ser identificado como tal.
d) Uma cláusula para a inclusão, se relevante, de um atributo específico do signatário, segundo os objetivos visados com a emissão do certificado;
e) Os dados de verificação de assinaturas correspondentes aos dados de criação de assinaturas que estejam sob o controlo do signatário
f) Identificação da data de início e de fim do prazo de validade do certificado
g) O código de identidade do certificado
h) A assinatura eletrônica avançada do prestador de serviços de certificação que o emite
i) As restrições ao âmbito de utilização do certificado, se for o caso; e
j) As restrições ao valor das transações nas quais o certificado pode ser utilizado, se for o caso.

– **Prestador de serviços de certificação:** entidade ou pessoa singular ou coletiva que emite certificados ou presta outros serviços relacionados com assinaturas eletrônicas.

AGIPRO

DIRECTIVA 1999/93/CE DO PARLAMENTO EUROPEU E DO CONSELHO

Acesso ao Mercado

– Os Estados-Membros não devem sujeitar a prestação de serviços de certificação a autorização prévia;

– Sem prejuízo do disposto no n.o 1, os Estados-Membros podem introduzir ou manter regimes de acreditação facultativos que se destinem a obter níveis mais elevados na oferta dos serviços de certificação

– Os Estados-Membros assegurarão a criação de um sistema adequado de controlo de prestadores de serviços de certificação

– A conformidade dos dispositivos seguros de criação de assinaturas é avaliada pelas entidades públicas ou privadas competentes designadas pelos Estados-Membros

– Os Estados-Membros e a Comissão cooperarão na promoção do desenvolvimento e utilização de dispositivos de verificação de assinaturas, à luz das recomendações relativas à verificação segura de assinaturas

– Os Estados-Membros podem submeter a utilização de assinaturas eletrônicas no sector público a eventuais requisitos adicionais.

DIRECTIVA 1999/93/CE DO PARLAMENTO EUROPEU E DO CONSELHO

Princípios relativos ao mercado interno e Efeitos Legais das Assinaturas Eletrônicas

– Estado-Membro: aplicará as disposições nacionais de acordo com a presente diretiva aos prestadores de serviços de certificação estabelecidos no seu território e aos serviços por eles prestados, não restringindo a prestação de serviços de certificação com origem em outro Estado-Membro nos domínios abrangidos pela presente diretiva.

– Os Estados-Membros assegurarão que os produtos de assinatura eletrônica que sejam conformes com a presente diretiva possam circular livremente no mercado interno.

–Efeitos Legais das assinaturas eletrônicas:

1) Os Estados-Membros assegurarão que as assinaturas eletrônicas avançadas baseadas num certificado qualificado e criadas através de dispositivos seguros de criação de assinaturas:
   a) Obedecem aos requisitos legais de uma assinatura no que se refere aos dados sob forma digital, do mesmo modo que uma assinatura manuscrita obedece àqueles requisitos em relação aos dados escritos; e
   b) São admissíveis como meio de prova para efeitos processuais.
2) Os Estados-Membros assegurarão que não sejam negados a uma assinatura eletrônica os efeitos legais e a admissibilidade como meio de prova para efeitos processuais apenas pelo fato de:
   a) se apresentar sob forma eletrônica,
   b) não se basear num certificado qualificado,
   c) não se basear num certificado qualificado emitido por um prestador de serviços de certificação acreditado,
   d) não ter sido criada através de um dispositivo seguro de criação de assinaturas.

AGIPRO

Responsabilidade e Aspectos Internacionais

– Os Estados-Membros assegurarão:

- ao emitir um certificado qualificado, um prestador de serviços de certificação seja responsável por prejuízos causados a qualquer entidade que confie no certificado qualificado;
- um prestador de serviços de certificação possa indicar no certificado qualificado:
  - os limites da sua utilização.
  - um limite para o valor das transações nas quais o certificado pode ser utilizado, desde que esse limite seja identificável por terceiros
- Serão propostos normas e acordos internacionais (bilaterais e multilaterais) para aceitação de normas de terceiros
- os certificados emitidos ao público, enquanto certificados qualificados, por um prestador de serviços de certificação estabelecido num país terceiro sejam considerados legalmente equivalentes aos certificados emitidos por um prestador de serviços de certificação estabelecido na Comunidade, desde que:
  a) O prestador de serviços de certificação obedeça aos requisitos constantes da presente diretiva e tenha sido acreditado sob um regime de acreditação facultativa vigente num Estado-Membro; ou
  b) O prestador de serviços de certificação estabelecido na Comunidade e que cumpre os requisitos da presente diretiva garanta o certificado; ou
  c) O certificado ou o prestador de serviços de certificação seja reconhecido com base num regime de acordo bilateral ou multilateral entre a Comunidade e países terceiros ou organizações internacionais.

Lei Modelo Uncitral

Lei modelo da Uncitral sobre assinatura Eletrônica (2001)

– Uncitral: Comissão das Nações Unidas para leis de comércio internacional

– Dividida em 2 partes:

- **Parte 1:** Lei Modelo da Uncitral sobre assinaturas eletrônicas
- **Parte2:** Guia para a aplicação da lei

– Convencidos de que a lei modelo sobre comércio eletrônico deu apoio significativo aos Estados facilitando a utilização do comércio eletrônico resultando na promulgação de leis em vários países.

– Cientes de novas tecnologias de identificação pessoal: assinaturas eletrônicas.

– Melhorar os princípios do art 7 da lei de comércio eletrônico (assinatura):

- Promover confiança em assinaturas eletrônicas para produção de efeitos jurídicos
- Assinaturas eletrônicas funcionalmente equivalentes a assinaturas manuscritas.

– harmonização de regras sobre o reconhecimento legal de assinaturas eletrônicas

– Modelo de Lei → Estados com diferentes sistemas jurídicos podem se ajustar harmoniosamente

– Recomenda Estados a seguir a lei quando promulgarem ou revisarem suas leis para uniformização da legislação.

Lei modelo da Uncitral sobre assinatura Eletrônica (2001) – Parte 1

– **Art 1:** Esfera de Aplicação

- uso de assinaturas eletrônicas no contexto de atividades comerciais

– **Art 2:** Definições

- **Assinatura Eletrônica:** dados em formato eletrônico apostos ou logicamente associados com a mensagem, que pode ser usado para identificar o signatário em relação a mensagem e os signatários de aprovação das informações contidas nas mensagens.

- **Certificado:** mensagem ou registro confirmando a ligação entre o signatário e assinatura

- **Prestador de serviços de certificação:** pessoa que emite certificados e pode prestar outros serviços relacionados com assinaturas eletrônicas.

– **Art 3:** Igualdade de tratamento das tecnologias de assinatura

1. Nenhuma disposição da presente Lei, exceto o artigo 5 º, deve ser aplicada de modo a excluir, restringir ou privar de efeito jurídico qualquer método de criação de uma assinatura eletrônica que satisfaz os requisitos do artigo 6 º, parágrafo 1, ou não atende aos requisitos da lei aplicável.

Lei modelo da Uncitral sobre assinatura Eletrônica (2001) – Parte 1

– **Art 4:** Interpretação

1. Lei de origem internacional para promover a uniformidade na sua aplicação e observância da boa fé.
2. Questões não resolvidas pela lei devem ser resolvidas em conformidade com os princípios gerais em que a lei é baseada.

– **Art 5:** Variação por acordo

1. As disposições da lei podem ser alteradas mediante acordo, a menos que o acordo não seja válido ou eficaz sobre a aplicação da lei.

– **Art 6:** Conformidade com a exigência de uma assinatura

1. Onde a lei requer a assinatura de uma pessoa, esta exigência é cumprida em relação a uma mensagem se a assinatura eletrônica usada é tão confiável quanto apropriado para a finalidade para a qual a mensagem foi gerada ou comunicada, à luz de todas as circunstâncias, incluindo qualquer acordo relevante.
2. O parágrafo 1 aplica-se se o requisito referido está na forma de uma obrigação ou se a lei simplesmente provê conseqüências para a ausência de uma assinatura.

Lei modelo da Uncitral sobre assinatura Eletrônica (2001) – Parte 1

– **Art 6:** Conformidade com a exigência de uma assinatura

3. Uma assinatura eletrônica é considerada confiável para satisfazer parágrafo 1 se:
   a) Os dados para criação da assinatura são ligados ao signatário e **a nenhuma outra pessoa**;
   b) Os dados para criação da assinatura estavam, no momento da assinatura, sob o controle de signatário e **de nenhuma outra pessoa;**
   c) Qualquer **alteração na assinatura eletrônica**, realizada depois da assinatura, é **detectável**;
   d) Onde o propósito da exigência legal de uma assinatura é prover garantias quanto a integridade da informação a que se refere, qualquer **alteração feita na informação** depois da assinatura, é **detectável**;
4. o parágrafo 3 não limita a capacidade de qualquer pessoa:
   a) Estabelecer de qualquer outra forma, com a finalidade de satisfazer o previsto no § 1 º, a confiabilidade de uma assinatura eletrônica;
   b) Fazer prova da não confiabilidade de uma assinatura eletrônica;
5. As disposições deste artigo não se aplicam ao seguinte.

– **Art 7:** Satisfação do Artigo 6

1. Qualquer pessoa, órgão ou autoridade, pública ou privada, especificado por decreto de Estado como competente pode determinar quais assinaturas eletrônicas cumprem o disposto no **art 6** desta lei.
2. Qualquer determinação feita nos termos do paragráfo 1 deve ser coerente com normas internacionais reconhecidas.
3. Este artigo não afeta o funcionamento das regras do direito internacional privado.

Lei modelo da Uncitral sobre assinatura Eletrônica (2001) – Parte 1

– **Art 8:** Conduta do Signatário:

1. Onde os dados de criação da assinatura eletrônica pode ser usado com efeito legal, o signatário deverá:

   a) Exercer cuidados razoáveis para evitar o uso não autorizado do dado de criação de sua assinatura;

   b) Sem demora indevida, utilizar os meios disponibilizados pelos **prestadores de serviço de certificação**, nos termos do **art 9** desta lei, ou usar esforços razoáveis, para notificar qualquer pessoa, se:

      i. O signatário sabe que o dado de criação de sua assinatura foi comprometido; ou

      ii. As circunstâncias conhecidas do signatário dá origem a um risco substancial que o dado de criação de sua assinatura pode ter sido comprometido.

   c) Quando um certificado é usado para apoiar a assinatura eletrônica, exercer cuidados razoáveis para assegurar a exatidão e integridade de todas as representações materiais feitas pelo signatário que são relevantes para o certificado durante todo o seu ciclo de vida ou que devem ser incluídas no certificado.

2. O signatário deve arcar com as conseqüências legais do seu fracasso em satisfazer os requisitos do parágrafo 1.

Lei modelo da Uncitral sobre assinatura Eletrônica (2001) – Parte 1

– **Art 9:** Conduta do Provedor de Serviço de Certificação:

1. Sempre que um prestador de serviços de certificação fornece serviços de apoio a assinatura eletrônica que pode ser utilizada para efeitos legais como uma assinatura, esse prestador de serviços de certificação deve:
   a) Agir de acordo com declarações feitas por ele com relação a suas políticas e práticas;
   b) exercer cuidados razoáveis para assegurar a exatidão e integridade de todas as representações materiais feitas por ele que são relevantes para o certificado durante todo o seu ciclo de vida ou que são incluídas no certificado.
   c) Proporcionar meios razoavelmente acessíveis que permitam uma terceira parte confiável verificar no certificado:
      i. A identidade do prestador de serviços de certificação
      ii. Que o signatário que é identificado no certificado tinha controle do **dado de criação da assinatura** no momento em que o certificado foi emitido.
      iii. Que os dados de criação da assinatura eram válidos no ou antes do tempo que o certificado foi emitido.
   d) Proporcionar meios razoavelmente acessíveis que permitam uma terceira parte confiável verificar no certificado, quando relevante, do certificado ou de maneira diferente:
      i. O método usado para identificar o signatário.
      ii. Qualquer restrição de propósito ou de valor que o dado de criação da assinatura ou o certificado podem ser usados.
      iii. Que os dados de criação da assinatura são válidos e não estão comprometidos.
      iv. Qualquer restrição ao âmbito ou extensão da responsabilidade prevista pelo provedor de serviços de certificação.
      v. Quais meios existem para o signatário notificar nos termos do **art 8**, paragráfo 1 desta lei.
      vi. Se um serviço de revogação é oferecido.

Lei modelo da Uncitral sobre assinatura Eletrônica (2001) – Parte 1

– **Art 9:** Conduta do Provedor de Serviço de Certificação:

e) Onde os serviços nos termos da alínea (d) (v) são oferecidos, proporcionar meios para que o signatário possa notificar nos termos do artigo 8, parágrafo 1 (b), desta Lei e, onde os serviços nos termos da alínea (d) (vi) são oferecidos, assegurar a disponibilidade de um serviço revogação;

f) Utilizar sistemas, procedimentos e recursos humanos confiáveis na realização de seus serviços.

2. Um prestador de serviços de certificação deve arcar com as conseqüências legais de seu fracasso para satisfazer os requisitos do parágrafo 1.

– **Art 10:** Confiabilidade:

1. Para os fins do **art 9**, parágrafo 1 (f), deve-se levar em contas os seguintes fatores:

a) Recursos financeiros e humanos, incluindo a existência de ativos;

b) Qualidade dos sistemas de hardware e software;

c) Procedimentos para o processamento de certificados e aplicações para certificados e retenção de registros;

d) Disponibilidade de informações para os signatários identificados nos certificados e possíveis terceiras partes confiáveis;

e) Regularidade e extensão da auditoria por uma entidade independente;

f) A existência de uma declaração do Estado, um organismo de acreditação ou do prestador de serviços de certificação quanto ao cumprimento ou existência do acima referido, ou

g) Qualquer outro fator relevante.

AGIPRO

Lei modelo da Uncitral sobre assinatura Eletrônica (2001) – Parte 1

– **Art 11:** Conduta da terceira parte de confiança:

1. A terceira parte confiável deve arcar com as conseqüências legais de suas falhas:
   a) Tomar medidas razoáveis para verificar a confiabilidade de uma assinatura eletrônica, ou;
   b) Onde uma assinatura eletrônica é suportada por um certificado, tomar medidas razoáveis:
      i. Para verificar a validade, suspensão ou revogação do certificado;
      ii. Para observar qualquer limitação que diz respeito ao certificado.

– **Art 12:** Reconhecimento de certificados e assinaturas eletrônicas estrangeiros :

1. Para determinar se, ou em que medida, um certificado ou uma assinatura eletrônica é juridicamente eficaz, não deverá ser considerado:
   a) À localização geográfica onde o certificado é emitido ou a assinatura eletrônica foi criada ou usada, ou;
   b) À localização geográfica do local de negócios do emissor ou signatários;
2. Um certificado digital emitido fora do Estado deve ter o mesmo efeito legal de um certificado digital emitido no Estado se ele oferece confiabilidade equivalente;
3. O mesmo deve ocorrer com a assinatura eletrônica criada fora do Estado;
4. Para ser determinar se um certificado digital ou uma assinatura eletrônica oferecem confiabilidade equivalente, deverá reconhecer às normas internacionais e quaisquer outros fatores relevantes;
5. Além dos parágrafos 2, 3 e 4, as partes concordam, entre si, usar certos tipos de assinaturas eletrônicas e certificados, que o concordantemente deve ser reconhecido como suficiente para os propósitos de reconhecimento transfronteiriços, a menos que o acordo não seja válido ou eficaz pela legislação aplicável.

Lei modelo da Uncitral sobre assinatura Eletrônica (2001) – Parte 2

– Guia para a Promulgação da Lei Modelo da UNCITRAL relativa às assinaturas eletrônicas:

- Ferramenta para Estados modernizarem suas legislações e também destinado para outros usuários, tais como juízes, árbitros, profissionais e acadêmicos.
- Aumento de técnicas de autenticação: quadro jurídico para reduzir incertezas.
- Abordagens legislativas diferentes em países X uniforme disposições legislativas.
- Igualdade de tratamento: usuários de computador X usuários do papel.
- Ambiente de mídia neutra e neutralidade tecnológica.
- Legislação nos países: inadequada ou desatualizada. Termos “escrito”, “assinado”, “original” → equivalência funcional.
- Evolução da Lei de comércio Eletrônico: incerteza da validade ou efeito legal.
- Evolução da Lei de comércio Eletrônico: assinatura digital e certificado digital.

Lei modelo da Uncitral sobre assinatura Eletrônica (2001) – Parte 2

– A Lei Modelo como uma ferramenta para harmonizar leis:

- Lei modelo está na forma de um texto legislativo que é recomendado aos Estados para incorporação em sua legislação nacional. Não interfere nas regras do direito internacional privado. Ao contrário de uma convenção internacional, não requer que os Estados notifiquem as Nações Unidas da promulgação de uma lei, mas são fortemente incentivados a informar a UNCITRAL de qualquer promulgação da nova lei modelo.

- Não é uma convenção: permite alterações no texto uniforme pelos Estados.

- Menor harmonização, no entanto, maior adesão. Mas pede-se mínimo de alteração possível.

- Alguns países acham que a lei modelo já é suficiente para resolver as questões jurídicas relacionadas a assinaturas eletrônicas.

- Baseada em PKI.

Lei modelo da Uncitral sobre assinatura Eletrônica (2001) – Parte 2

– Observações gerais sobre assinatura eletrônica:

- **Em mensagens eletrônicas o original é indistinguível da cópia, não tem uma assinatura manuscrita e não está no papel.**
- Potencial de fraude é considerável se usar tecnologias inadequadas.
- Análise de várias técnicas para **fornecer equivalentes funcionais para assinaturas manuscritas** e outros tipos de mecanismos de autenticação usados no papel, como por exemplo, selos ou carimbos.
- Decisão de focar em PKI: relações entre signatários, provedores de serviço de certificação e terceiras partes confiáveis.
- Outros dispositivos são cobertos no conceito de assinatura eletrônica: botão de ok, assinatura manuscrita em um dispositivo biométrico, etc..
- A UNCITRAL :
  - intenção de desenvolver uma legislação uniforme para ambos tipos de assinatura,
  - especificidade de uso de cada técnica
  - não quer desencorajar o uso de qualquer método:neutralidade de mídia.
- Muitos países estão usando a assinatura digital que usa a criptografia de chaves públicas.
- Define o que é assinatura digital, chave pública, chave privada, algoritmo de hash e cita algoritmos de assinatura, como RSA e curvas elípticas. Exemplifica a assinatura e a verificação da assinatura e o papel do provedor de serviço de certificação.
- Um signatário pode emitir uma declaração pública indicando que as assinaturas verificáveis por sua chave pública podem ser tratadas como original. A forma e eficácia jurídica da declaração deve ser regida pela lei do Estado. Muitas vezes é usada a PKI.

Lei modelo da Uncitral sobre assinatura Eletrônica (2001) – Parte 2

– Principais características da Lei Modelo:

- Derivada do **art 7** da Lei Modelo UNCITRAL de comércio Eletrônico:
  - Detalha método confiável para identificar uma pessoa
  - Detalha método confiável de indicar a aprovação desta pessoa sobre a informação contida na mensagem.
- Pensou-se em: definir regras contratuais, disposições legislativas ou diretrizes
- Definiu-se criar um conjunto de regras legislativas com comentários.
- Total consistência com lei modelo de comércio eletrônico.
  - Conceitos, Neutralidade de mídia e indiscriminação da equivalência funcional dos tradicionais conceitos e práticas da abordagem em papel.
- Aplicabilidade:
  - Ambiente aberto: as partes se comunicam eletronicamente sem acordo prévio.
  - Ambiente fechado: como disposições de modelo contratual ou regras padrão onde as partes estão sujeitas a regras contratuais e procedimento pré-existentes a serem seguidos na comunicação eletrônica.

Lei modelo da Uncitral sobre assinatura Eletrônica (2001) – Parte 2

– Principais características da Lei Modelo:

- A palavra “lei” não refere-se apenas a lei estatutária ou regulamentar mas também as regras de direito criadas por resoluções judiciais e outras formas de direito processual. O sentido é amplo pois a maioria dos documentos será confrontado com o direito da prova em matéria de prova por escrito.
- Regras para ser completadas por regulamentos técnicos e contrato:
  - O estado pode ampliar a lei sem comprometer seu objetivo.
  - A lei não cobre todos os aspectos do uso de assinaturas eletrônicas.
  - Recomenda-se manter a flexibilidade na operação da assinatura eletrônica.
  - A prática comercial tem uma dependência de longa data sobre o processo de padronização técnica. Usar padrões abertos e interoperáveis para apoiar o reconhecimento transacional .
  - Os procedimentos e implementações de normas técnicas da assinatura digital não são encontrados na lei modelo.
  - Outros organismos de direito podem incluir:
    - Aplicabilidade em contratos administrativos.
    - Responsabilidades civis e criminais.
    - Lei de Processo judicial.

Lei modelo da Uncitral sobre assinatura Eletrônica (2001) – Parte 2

– Principais características da Lei Modelo:

- Adoção de um conjunto de critérios flexíveis para o reconhecimento de um assinatura eletrônica como funcionalmente equivalente a uma assinatura manuscrita.
- Estabelece condições gerais para que as mensagens sejam consideradas autenticadas com credibilidade suficiente para que não tenham seu valor legal negado. (barreiras com autenticações fracas)
- ... O método utilizado deve ser tão confiável quanto é apropriado para a finalidade para a qual a mensagem de dados é gerada ou comunicada, à luz de todas as circunstâncias, incluindo qualquer acordo entre o remetente e o destinatário da mensagem de dados.
- Para determinar se o método é apropriado, fatores jurídicos, técnicos e comerciais podem ser considerados:
  - Sofisticação dos equipamentos utilizados.
  - A natureza da atividade comercial.
  - A freqüência com que ocorre transações comerciais entre as partes
  - O tipo e o tamanho da operação.
  - A função de requisitos de assinatura em um determinado ambiente legal e regulatório.
  - A capacidade dos sistemas de comunicação.
  - A conformidade dos procedimentos de autenticação definido com intermediários.
  - A gama de procedimentos de autenticação disponíveis por qualquer intermediário.
  - A conformidade com os costumes e práticas comerciais.
  - A existência de mecanismos de cobertura de seguro contra mensagens não autorizadas
  - A importância e o valor das informações contidas na mensagem de dados.
  - A existência e a disponibilidade de métodos alternativos de identificação e o custo de implementação.
  - o grau de aceitação ou não aceitação do método de identificação na indústria relevante ou campo, tanto no momento em que o método foi acordado e o momento em que a mensagem de dados foi comunicada.
  - Qualquer outro fator relevante.

AGIPRO

Lei modelo da Uncitral sobre assinatura Eletrônica (2001) – Parte 2

– Principais características da Lei Modelo:

- Estabelece mecanismo para que assinaturas eletrônicas que cumpram critérios técnicos de confiabilidade possam ser criadas com pré-determinação de seu valor legal .
- Dependendo do momento em que a certeza é alcançado quanto ao reconhecimento de uma assinatura electrônica como funcionalmente equivalente a uma assinatura manuscrita, a Lei Modelo estabelece dois regimes distintos.
  - O primeiro e mais amplo é o descrito no artigo 7 º da Lei Modelo da UNCITRAL sobre Comércio Eletrônico. Ele reconhece qualquer "método" que pode ser utilizados para cumprir uma exigência legal para a assinatura manuscrita. A eficácia jurídica de tal "método" como um equivalente a uma assinatura manuscrita depende de demonstração de sua "confiança" a um julgador de fato.
  - O segundo e mais estreito que é criado pela nova Lei Modelo contempla métodos de assinatura eletrônica que pode ser reconhecida por uma autoridade do Estado, uma entidade privada credenciada, ou as próprias partes, como satisfazendo os critérios de confiabilidade técnica estabelecidos na Lei Modelo. A vantagem desse reconhecimento é que traz a certeza para os usuários de que tais técnicas de assinatura eletrônica são confiáveis antes que eles realmente usem a técnica.

Lei modelo da Uncitral sobre assinatura Eletrônica (2001) – Parte 2

– Principais características da Lei Modelo:

- A lei modelo não trata em detalhes as responsabilidades que podem afetar as várias partes envolvidas na operação de assinatura eletrônica. Estas devem ser tratadas em outra lei. Entretanto a lei modelo determina critérios que fixam a conduta das partes (signatário, provedor de serviço de certificação e parte que confia na assinatura).
- O signatário deve ter cuidado razoável para o dado de criação da assinatura eletrônica (chave privada). Deve evitar uso não autorizado. A assinatura digital, por ela própria, não garante que quem assinou o documento foi o signatário. Se a chave foi comprometida, o signatário deve avisar o provedor de serviços.
- A parte que confia na assinatura cabe realizar os passos razoáveis para verificar a confiança da assinatura e do certificado usado na assinatura.
- O provedor de serviços de certificação deve usar sistemas confiáveis, recursos humanos e procedimentos de acordo com políticas e práticas definidas. Assegurar a precisão e a completude das informações dos certificados . Além disso deve:
  - Garantir a ligação entre o signatário e o certificado e que o signatário tem a chave privada do mesmo.
  - A chave privada foi emitida antes do certificado.
  - Identificação do signatário na emissão, de possíveis limitadores de propósito, e do escopo de uso, permitir formas de informar o comprometimento das chaves e oferecer um serviço de revogação.

Lei modelo da Uncitral sobre assinatura Eletrônica (2001) – Parte 2

– Principais características da Lei Modelo:

- A lei modelo prove critério de reconhecimento legal de assinatura eletrônica independente da tecnologia usada:
  - Certificados digitais baseado em criptografia assimétrica.
  - Dispositivos biométricos
  - Criptografia simétrica
  - Uso de senhas
  - Uso de tokens
  - Versões digitalizadas da assinatura manuscrita
  - Botão OK.
- A combinação destas tecnologias deve ser usada para reduzir o risco do sistema.
- A lei modelo estabelece um princípio básico de que não importa onde a assinatura ou o certificado foi criado, mas a segurança das técnicas usadas para emissão.
- UNCITRAL Model Law on International Commercial Arbitration
- UNCITRAL Model Law on International Credit Transfers
- UNCITRAL Model Law on Procurement of Goods, Construction and Services
- UNCITRAL Model Law on Electronic Commerce
- UNCITRAL Model Law on Cross-Border Insolvency

Leis em outros Países

Países que possuem leis de assinatura digital

- Alemanha
- Argentina
- Chile
- China
- Colômbia
- Eslováquia
- Espanha
- Estados Unidos da América
- França
- Grécia
- Itália
- Peru
- Portugal
- Reino Unido
- Venezuela
- outros...

Documentos importantes no mercosul

- **Tratado de Assunção (1991)**
  - criação de um mercado comum entre Brasil, Argentina, Paraguai e Uruguai.

- **Protocolo de Ouro Preto (1994)**
  - Estabelece as bases institucionais do MERCOSUL.

- **MERCOSUR/GMC/RES. Nº 22/04**
  - USO DE FIRMA DIGITAL EN EL ÁMBITO DE LA SECRETARÍA DEL MERCOSUR

- **MERCOSUR/GMC EXT./RES. Nº 34/06**
  - DIRECTRICES PARA LA CELEBRACIÓN DE ACUERDOS DE RECONOCIMIENTO MUTUO DE FIRMAS ELECTRÓNICAS AVANZADAS EN EL ÁMBITO DEL MERCOSUR

- MERCOSUR/GMC EXT./RES. Nº 37/06
  - RECONOCIMIENTO DE LA EFICACIA JURÍDICA DEL DOCUMENTO ELECTRÓNICO, LA FIRMA ELECTRÓNICA Y LA FIRMA ELECTRÓNICA AVANZADA EN EL ÁMBITO DEL MERCOSUR

PROVA

Conceito de Prova

– No direito processual, provar resume-se na realização de uma tarefa necessária e obrigatória, **para constituir estado de convencimento** no espírito do juiz, este na condição de órgão julgador, **a respeito de um fato alegado** e sua efetiva ocorrência, tal como foi descrito. Prova, assim, é meio, é instrumento utilizado para a **demonstração da realidade** material. De modo a criar, no espírito humano, **convencimento** de adequação. **Prova judiciária**, por seu turno, é o meio **demonstrativo de veracidade entre o fato material** (fato constitutivo do direito) **e o fundamento jurídico do pedido**. Vale dizer é o meio pelo qual se estabelece relação de veracidade e adequação entre a causa próxima e a causa remota, elementos da causa de pedir. Estabelecida a relação, por meio da prova, ao juiz é dada a tarefa de aplicar a lei, a hipótese normativa de incidência fática, em regra, a norma de direito material. (Aclibes Burgarelli)

Forma da Prova

– **Prova Testemunhal**, em sentido amplo, é a afirmação pessoal oral. No quadro das provas testemunhais, ou orais, se compreendem as produzidas por testemunha, depoimento de parte, confissão, juramento. **Prova Material** é a consistente em qualquer materialidade que sirva de prova do fato probando; é a atestação emanada da coisa: o corpo de delito, os exames periciais etc. Por fim, a **prova Documental** é a afirmação escrita ou gravada: as escrituras públicas ou particulares, cartas missivas, plantas, projetos, desenhos, fotografias, etc. (Moacyr Amaral Santos)

– A prova testemunhal é em geral a verificação de pessoas na forma real ou possível; A prova material é a verificação de coisa na materialidade das suas formas; **A prova documental é a verificação na forma do escrito ou de outra materialidade permanente**. (Nicola Framarino de MALATESTA)

AGIPRO

Conceitos de Documento

O documento

– Qualquer base de conhecimento, fixada materialmente e disposta de maneira que se possa utilizar para consulta, estudo, prova, etc. (Aurélio)

– A prova histórica real consistente na representação física de um fato. (José Frederico Marques).

– documento, em sentido amplo, é toda representação material destinada a reproduzir determinada manifestação do pensamento, como uma voz fixada duradouramente (vox mortua). (Giuseppe Chiovenda)

– "a coisa representativa de um fato e destinada a fixá-lo de modo permanente e idôneo, reproduzindo-o em juízo" (Moacyr Amaral Santos).

– Francesco Carnelutti diz que "a configuração do verdadeiro documento independe do meio em que aquele está armazenado, sendo mais relevante que ele seja a representação de uma idéia ou de um fato que se pretende perpetuar"

O documento eletrônico

– Uma seqüência de bits que, traduzida por meio de um determinado programa de computador, seja representativa de um fato. Da mesma forma que os documentos físicos, o documento eletrônico não se resume em escritos: pode ser um texto escrito, como também pode ser desenho, uma fotografia digitalizada, sons, vídeos, enfim, tudo que puder representar um fato e que esteja armazenado em um arquivo digital. (Marcacini).

– "Pode-se dizer que experimentamos hoje um mundo virtual onde, no lugar de átomos, agora temos que nos acostumar com uma realidade de coisas formadas tanto por átomos como por bits. O documento tradicional, em nível microscópico, não é outra coisa senão uma infinidade de átomos que, juntos, formam uma coisa que, captada pelos nossos sentidos, nos transmite uma informação. O documento eletrônico, então, é uma das seqüências de bits que, captada pelos nossos sentidos com o uso de um computador e um software específico, nos transmite uma informação. (Nicholas Negroponte)

AGIPRO

Requisitos Necessários

– Autenticidade

– Integridade

– Tempestividade

– Perenidade de conteúdo

- validade da informação ou do conteúdo ao longo do tempo;
- forma de armazenamento;

– Força Probatória (CPC):

- Art. 383. Qualquer reprodução mecânica, como a fotográfica, cinematográfica, fonográfica ou de outra espécie, faz prova dos fatos ou das coisas representadas, se aquele contra quem foi produzida lhe admitir a conformidade.

- Parágrafo único. Impugnada a autenticidade da reprodução mecânica, o juiz ordenará a realização de **exame pericial**.

Validade jurídica dos Documentos

MP 2.200-2 de 24 de Agosto de 2001

– **Art 1º** Institui a Infraestrutura 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 3º** A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares...

– **Art 4º** Define as competências do Comitê Gestor da ICP-Brasil

– **Art. 5º** À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.

AGIPRO

MP 2.200-2 de 24 de Agosto de 2001

– **Art. 5º** À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.

– **Art. 10º** 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 verdadeiros 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.

– **Art. 11º** A utilização de documento eletrônico para fins tributários atenderá, ainda, ao disposto no art. 100 da Lei nº 5.172, de 25 de outubro de 1966 - Código Tributário Nacional.

– **Art. 13º** O ITI é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira.

AGIPRO

Lei 11.280/2006 e Lei 11.419/2006

– Alteração do Código de Processo Civil (Leis 11.280/2006 11.419/2006)

- Art. 154. Os atos e termos processuais não dependem de forma determinada senão quando a lei expressamente a exigir, reputando-se válidos os que, realizados de outro modo, lhe preencham a finalidade essencial.

  Parágrafo único. Os tribunais, no âmbito da respectiva jurisdição, poderão disciplinar a prática e a comunicação oficial dos atos processuais por meios eletrônicos, atendidos os requisitos de autenticidade, integridade, validade jurídica e interoperabilidade da Infra-Estrutura de Chaves Públicas Brasileira - ICP - Brasil. (Incluído pela Lei nº 11.280, de 2006)

  § 2o Todos os atos e termos do processo podem ser produzidos, transmitidos, armazenados e assinados por meio eletrônico, na forma da lei. (Incluído pela Lei nº 11.419, de 2006).

– Lei 11.419/2006

- Dispõe sobre a informatização do Processo Judicial
- Permite a comunicação eletrônica dos Atos Processuais (Diário de Justiça Eletrônico)
- Define as regras do processo eletrônico no judiciário
  - Fomentou o uso de documentos eletrônicos nos processos e serviu de diretriz para as demais legislações que tratam de processo eletrônico no País.

Legislação Pertinente

– 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.

– DECRETO Nº 3.872, DE 18 DE JULHO DE 2001

- Dispõe sobre o Comitê Gestor da InfraEstrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva, sua Comissão Técnica Executiva 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.

– DECRETO Nº 4.414, DE 07 DE OUTUBRO DE 2002

- Altera o decreto 3.996 de 2001

–PROJETO DE LEI Nº 7.316, de 07 de Novembro de 2002

- Disciplina o uso de assinaturas eletrônicas e a prestação de serviços de certificação.

Outras Leis Nacionais

Legislação Pertinente

– LEI Nº. 12.333, DE 23 DE JANEIRO DE 2003.

- Estabelece a escrituração fiscal digital para contribuintes do ICMS.

– DECRETO Nº 4.689, DE 07 DE MAIO DE 2003

- Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Instituto Nacional de Tecnologia da Informação - ITI, e dá outras providências.

– LEI No 10.740, DE 1º DE OUTUBRO DE 2003.

- Altera a Lei no 9.504, de 30 de setembro de 1997, e a Lei no10.408, de 10 de janeiro de 2002, para implantar o registro digital do voto.

– DECRETO Nº 25.223, DE 15 DE OUTUBRO DE 2004

- Institui o Serviço Interativo de Atendimento Virtual - Agênci@Net, que estabelece a obrigatoriedade de entrega de informações econômico fiscais e documentos eletrônicos com aposição de assinatura digital, e dá outras providências.

– DECRETO Nº. 15.059, de 27 de janeiro de 2006

- Normatiza a Escrituração Eletrônica mensal do livro fiscal e a Declaração Eletrônico Anual ser realizada por meio do "software" ISSQNDec e dá outras providências.

AGIPRO

Outras Leis Nacionais

Legislação Pertinente

– DECRETO Nº 6.022, DE 22 DE JANEIRO DE 2007.

- Institui o Sistema Público de Escrituração Digital – Sped

– DECRETO Nº 6.605, DE 14 DE OUTUBRO DE 2008

- Dispõe sobre o Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva - COTEC.

– LEI Nº 12.682, DE 9 DE JULHO DE 2012.

- Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos.

– Carta Circular 3134 – Banco Central do Brasil

- Divulga os procedimentos e padrões técnicos para uso de a assinatura digital em contratos de câmbio.

– CIRCULAR 3.234 do Banco Central do Brasil

- Altera a regulamentação cambial para prever a assinatura digital em contratos de câmbio por meio da utilização de certificados digitais emitidos no âmbito da Infraestrutura de Chaves Públicas (ICP-Brasil), e dá outras providências.

Outras Leis Nacionais

Legislação Pertinente

–CIRCULAR SUSEP Nº. 277, de 30 de novembro de 2004.

- Faculta a utilização da assinatura digital, nos documentos eletrônicos relativos às operações de seguros, de capitalização e de previdência complementar aberta, por meio de certificados digitais emitidos no âmbito da Infraestrutura de Chaves Públicas (ICP-Brasil), e dá outras providências.

–RESOLUÇÃO CFM Nº. 1.821/07

- Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde.

– Instruções Normativas , Portarias, Resoluções e documentos principais da ICP-Brasil

– Instruções Normativas ICP-Brasil

– Entre outras.

ICP- BRASIL

- O que é a ICP-Brasil?
- Como funciona?
- Estrutura da ICP-Brasil
- Principais documentos
  - Documentos Principais - DOC – ICPs
  - Manuais de Condutas Técnicas
  - Resoluções

ICP-BRASIL

O que é a ICP-Brasil?

– A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Observa-se que o modelo adotado pelo Brasil foi o de certificação com raiz única, sendo que o ITI, além de desempenhar o papel de Autoridade Certificadora Raiz (AC-Raiz), também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

Como funciona a ICP-Brasil?

– AC-RAIZ

- a Autoridade Certificadora Raiz da ICP-Brasil (AC-Raiz) é a primeira autoridade da cadeia de certificação. Executa as Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil.

– AC – Autoridade Certificadora

- Uma Autoridade Certificadora (AC) é uma entidade, pública ou privada, subordinada à hierarquia da ICP-Brasil, responsável por emitir, distribuir, renovar, revogar e gerenciar certificados digitais.

– AR – Autoridade de Registro

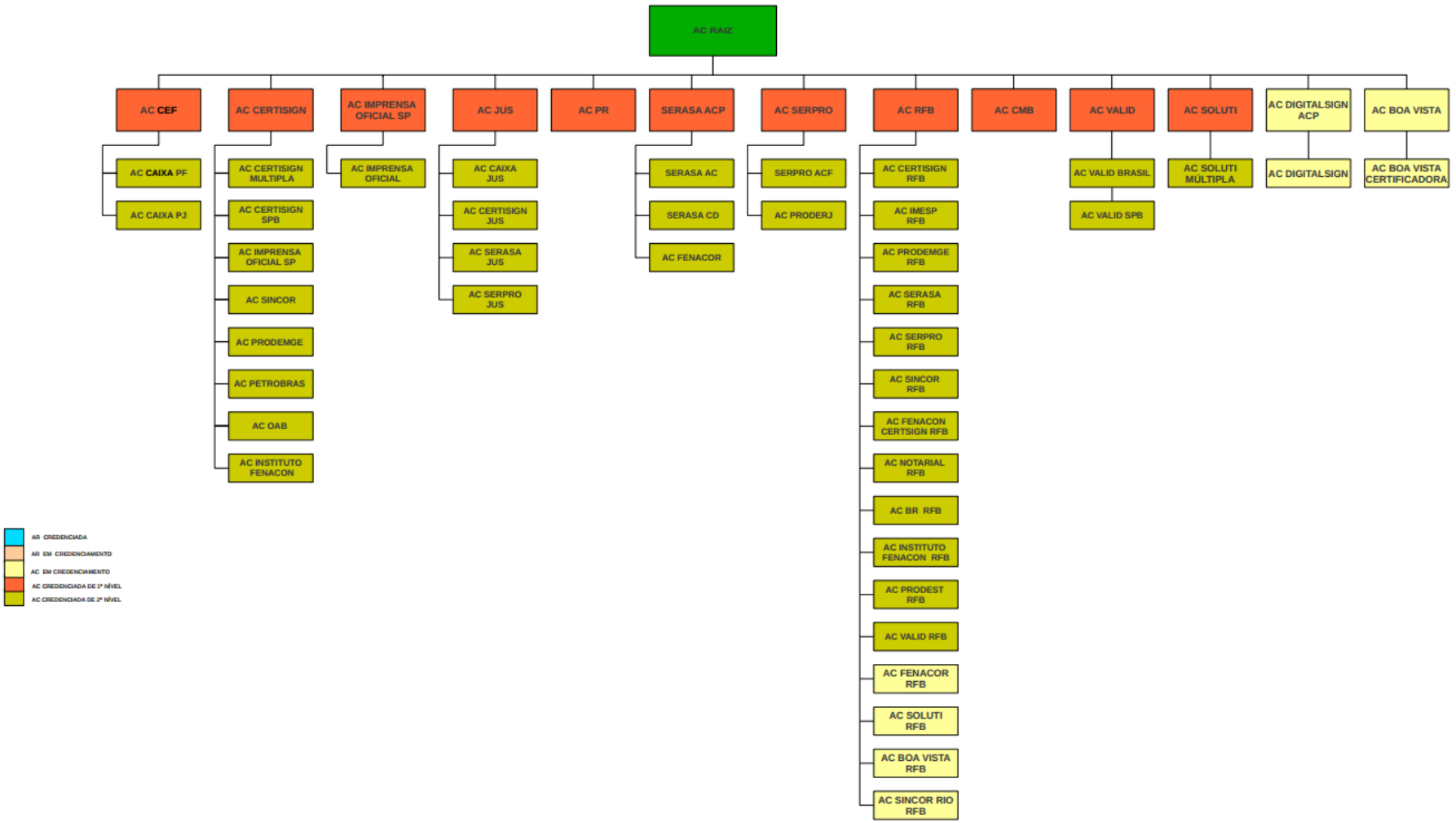
- Uma Autoridade de Registro (AR) é responsável pela interface entre o usuário e a Autoridade Certificadora. Vinculada a uma AC, tem por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais e identificação, de forma presencial, de seus solicitantes.

– ACT – Autoridade de Carimbo do Tempo

- Uma Autoridade Certificadora do Tempo (ACT) é uma entidade na qual os usuários de serviços de Carimbo do Tempo confiam para emitir Carimbos do Tempo.

AGIPRO

Estrutura da ICP-Brasil?



Principais Documentos da ICP-Brasil

Documentos Principais

– DOC-ICP-01
- DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL.

– DOC-ICP-01.01
- PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL - V.2.3

–DOC-ICP-02
- POLÍTICA DE SEGURANÇA DA ICP-BRASIL - V.3.0

– DOC-ICP-03
- CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL - V4.6

– DOC-ICP-03.01
- CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL - V1.6

– DOC-ICP-04
- REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL - V.5.1

– DOC-ICP-04.01
- ATRIBUIÇÃO DE OID NA ICP-BRASIL - V.2.3

Principais Documentos da ICP-Brasil

Documentos Principais

– DOC-ICP-05

- REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL - V.3.6

– DOC-ICP-05.01

- PROCEDIMENTOS DE IDENTIFICAÇÃO DE SERVIDORES DO SERVIÇO EXTERIOR BRASILEIRO EM MISSÃO PERMANENTE NO EXTERIOR - V.1.

–DOC-ICP-06

- POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL - V.3.0

– DOC-ICP-07

- DIRETRIZES PARA SINCRONIZAÇÃO DE FREQÜÊNCIA E DE TEMPO NA INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA - ICP-BRASIL - V.1.0

– DOC-ICP-08

- CRITÉRIOS E PROCEDIMENTOS PARA AUDITORIA DAS ENTIDADES INTEGRANTES DA ICP-BRASIL - V.4.0

– DOC-ICP-09

- CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL - V.3.0

AGIPRO

Principais Documentos da ICP-Brasil

Documentos Principais

– DOC-ICP-10
  - REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL - V.3.0

– DOC-ICP-10.1
  - PROCEDIMENTOS ADMINISTRATIVOS PARA HOMOLOGAÇÃO NA ICP-BRASIL - V.3.2

– DOC-ICP-10.2
  - ESTRUTURA NORMATIVA TÉCNICA E NÍVEIS DE SEGURANÇA DE HOMOLOGAÇÃO A SEREM UTILIZADOS NOS PROCESSOS DE HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL - V.3.0

– DOC-ICP-10.3
  - PADRÕES E PROCEDIMENTOS TÉCNICOS A SEREM OBSERVADOS NOS PROCESSOS DE HOMOLOGAÇÃO DE CARTÕES INTELIGENTES, (SMART CARDS), LEITORAS DE CARTÕES INTELIGENTES E TOKENS CRIPTOGRÁFICOS NO ÂMBITO DA ICP-BRASIL - V.3.0

– DOC-ICP-10.4
  - PADRÕES E PROCEDIMENTOS TÉCNICOS A SEREM OBSERVADOS NOS PROCESSOS DE HOMOLOGAÇÃO DE SOFTWARES DE ASSINATURA DIGITAL,SIGILO E AUTENTICAÇÃO NO ÂMBITO DA ICP-BRASIL - V.2.0

– DOC-ICP-10.5
  - PADRÕES E PROCEDIMENTOS TÉCNICOS A SEREM OBSERVADOS NOS PROCESSOS DE HOMOLOGAÇÃO DE MÓDULOS DE SEGURANÇA CRIPTOGRÁFICA (MSC)NO ÂMBITO DA ICP-BRASIL - V.1.0

– DOC-ICP-10.6
  - PADRÕES E PROCEDIMENTOS TÉCNICOS A SEREM OBSERVADOS NOS PROCESSOS DE HOMOLOGAÇÃO DE SOFTWARES DE BIBLIOTECAS CRIPTOGRÁFICASE SOFTWARES PROVEDORES DE SERVIÇOS CRIPTOGRÁFICOS NO ÂMBITO DA ICP-BRASIL - V.1.0

– DOC-ICP-10.7
  - CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DE LABORATÓRIOS DE ENSAIOS E AUDITORIA INTEGRANTES ICP-BRASIL- V.1.0

AGIPRO

Principais Documentos da ICP-Brasil

Documentos Principais

– DOC-ICP-11
- VISÃO GERAL DO SISTEMA DE CARIMBOS DO TEMPO NA ICP-BRASIL - V.1.2

– DOC-ICP-12
- REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL - V.1.1

–DOC-ICP-13
- REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO DA ICP-BRASIL - V.1.1

– DOC-ICP-14
- PROCEDIMENTOS PARA AUDITORIA DO TEMPO DA ICP-BRASIL - V.1.1

– DOC-ICP-15
- VISÃO GERAL SOBRE ASSINATURAS DIGITAIS NA ICP-BRASIL - V.2.1

– DOC-ICP-15.01
- REQUISITOS MÍNIMOS PARA GERAÇÃO E VERIFICAÇÃO DE ASSINATURAS DIGITAIS NA ICP-BRASIL - V.2.1

– DOC-ICP-15.02
- PERFIL DE USO GERAL PARA ASSINATURAS DIGITAIS NA ICP-BRASIL - V.2.1

– DOC-ICP-15.03
- REQUISITOS DAS POLÍTICAS DE ASSINATURA DIGITAL NA ICP-BRASIL - V.6.1

AGIPRO

Principais Documentos da ICP-Brasil

Documentos Principais

– DOC-ICP-16
  - VISÃO GERAL SOBRE CERTIFICADO DE ATRIBUTO PARA A ICP-BRASIL - V.1.0

– DOC-ICP-16.01
  - PERFIL DE USO GERAL E REQUISITOS PARA GERAÇÃO E VERIFICAÇÃO DE CERTIFICADOS DE ATRIBUTO NA ICP-BRASIL - V.1.0

Manuais de Conduta Técnica

– MCT 1
  - Volume I - Requisitos Materiais Documentos Cartões
  - Volume II - Procedimentos Ensaios Homologação Cartões

– MCT2
  - Volume I - Requisitos Materiais Documentos Leitoras
  - Volume II - Procedimentos Ensaios Homologação Leitoras

– MCT 3
  - Volume I - Requisitos Materiais Documentos Tokens
  - Volume II - Procedimentos Ensaios Homologação Tokens

Manuais de Conduta Técnica

- MCT 4
  - Volume I - Requisitos Materiais Documentos para Softwares de Assinatura
  - Volume II - Procedimentos Ensaios Homologação Softwares de Assinatura

- MCT 5
  - Volume I - Requisitos Materiais Documentos para Softwares de Autenticação
  - Volume II - Procedimentos Ensaios Softwares de Autenticação

- MCT 6
  - Volume I - Requisitos Materiais Documentos para Softwares de Sigilo
  - Volume II - Procedimentos Ensaios para Softwares de Sigilo

- MCT 7
  - Volume I - Requisitos, Materiais e Documentos Homologação de MSC
  - Volume II - Procedimentos Ensaios Homologação de MSC

- MCT 8
  - Volume I - Requisitos, Materiais e Documentos Homologação Bibliotecas Criptográficas
  - Volume II - Procedimentos Ensaios Homologação Bibliotecas Criptográficas

Manuais de Conduta Técnica

- MCT 9
  - Volume I - Requisitos, Materiais e Documentos Homologação Softwares CSP
  - Volume II - Procedimentos Ensaios Homologação Softwares CSP

- MCT 10
  - Volume I -Requisitos, Materiais e Documentos Técnicos para Homologação de Carimbo do Tempo no âmbito da ICP-Brasil
  - Volume II - Procedimentos Ensaios Carimbo de Tempo no âmbito da ICP-Brasil

- MCT 11
  - Volume I -Procedimentos de Ensaios para Avaliação de Conformidade aos Requisitos Técnicos de Softwares de AC e AR no âmbito da ICP-Brasil
  - Volume II -Procedimentos de Ensaios para Avaliação de Conformidade aos Requisitos Técnicos de Softwares de AC e AR no âmbito da ICP-Brasil

Principais Documentos da ICP-Brasil

Resoluções

Resolução	Descrição
Resolução nº 3	Designa Comissão para auditar a Autoridade Certificadora Raiz - AC Raiz e seus prestadores de serviços.
Resolução nº 5	Aprova o Relatório de auditoria da AC Raiz.
Resolução nº 15	Estabelece as diretrizes para sincronização de frequência e de tempo na Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.
Resolução nº 16	Estabelece as diretrizes para sincronização de frequência e de tempo na Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.
Resolução nº 20	Determina o desenvolvimento de uma plataforma criptográfica aberta, voltada à operação da AC Raiz.
Resolução nº 29	Designar a seguinte Comissão para realizar auditoria pré-operacional da AC Raiz
Resolução nº 33	Delega a AC RAIZ da ICP-Brasil atribuição para suplementar as normas do Comitê Gestor e dá outras providências.
Resolução nº 39	Aprova a versão 2.0 da Política de Segurança da ICP-Brasil.
Resolução nº 41	Aprova a versão 2.0 dos Requisitos Mínimos para as POLÍTICAS DE CERTIFICADO na ICP-Brasil.
Resolução nº 42	Aprova a versão 2.0 dos Requisitos Mínimos para as DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO das Autoridades Certificadoras da ICP-Brasil.
Resolução nº 44	Aprova a versão 2.0 dos Critérios e Procedimentos para Realização de AUDITORIAS NAS ENTIDADES nas Entidades da ICP-Brasil.
Resolução nº 45	Aprova a versão 2.0 dos Critérios e Procedimentos para FISCALIZAÇÃO das Entidades Integrantes da ICP-Brasil.
Resolução nº 47	Aprova a versão 3.0 dos Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil.
Resolução nº 48	Altera os Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil.

AGIPRO

Principais Documentos da ICP-Brasil

Resoluções

Resolução	Descrição
Resolução nº 49	Aprova a versão 3.0 da Declaração de Práticas de Certificação da Autoridade certificadora Raiz da ICP-Brasil.
Retificação da Resolução nº 49	
Resolução nº 50	Altera a Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil.
Resolução nº 51	Altera a Política de Segurança da ICP-Brasil.
Resolução nº 52	Altera os critérios e procedimentos para credenciamento das entidades integrantes da ICP-Brasil.
Retificação da Resolução nº 52	
Resolução nº 53	Altera os requisitos mínimos para as políticas de certificado na ICP-Brasil.
Retificação da Resolução nº 53	
Resolução nº 54	Altera os requisitos mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil.
Resolução nº 55	Aprova a versão 3.0 das diretrizes da política tarifária da Autoridade Certificadora Raiz da ICP-Brasil.
Resolução nº 56	Altera os critérios e procedimentos para realização de auditorias nas entidades da ICP-Brasil.
Retificação da Resolução nº 56	
Resolução nº 57	Altera os critérios e procedimentos para fiscalização das entidades integrantes da ICP-Brasil.
Retificação da Resolução nº 57	
Resolução nº 58	Aprova a versão 1.0 do documento Visão Geral do Sistema de Carimbos do Tempo na ICP-Brasil.

AGIPRO

Principais Documentos da ICP-Brasil

Resoluções

Resolução	Descrição
Resolução nº 59	Aprova a versão 1.0 do documento Requisitos Mínimos para as Declarações de Práticas das Autoridades de Carimbo do Tempo da ICP-Brasil.
Resolução nº 60	Aprova a versão 1.0 do documento Requisitos Mínimos para as Políticas de Carimbo do Tempo da ICP-Brasil.
Resolução nº 61	Aprova a versão 1.0 do documento Procedimentos para Auditoria do Tempo na ICP-Brasil.
Resolução nº 62	Aprova a versão 1.0 do documento Visão Geral sobre Assinaturas Digitais na ICP-Brasil.
Resolução nº 63	Aprova o Regimento Interno do Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).
Resolução nº 64	Aprova a execução de auditoria no ambiente operacional na Autoridade Certificadora raiz (AC RAIZ) e seus prestadores de serviço de suporte de INFRA - ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA no exercício de 2010.
Resolução nº 65	Aprova a Versão 2.0 do documento padrões e algoritmo criptográficos da ICP-BRASIL, e o plano de migração relacionado.
Resolução nº 66	Aprova a Versão 3.1 dos requisitos mínimos para a declaração de práticas de certificação das autoridades certificadoras da ICP-Brasil.
Resolução nº 67	Aprova a Versão 3.1 dos requisitos mínimos para a declaração de práticas de certificação das autoridades certificadoras da ICP-Brasil.
Resolução nº 68	Altera os prazos contidos no plano de adoção de novos padrões criptográficos - anexo II da resolução Nº 65.
Resolução nº 69	Aprova a versão 1.1 dos normativos de carimbo de tempo da ICP-Brasil.
Resolução nº 70	Aprova a versão 4.2 DOC-ICP-03.
Resolução nº 71	Altera o prazo da resolução 62 REF DOC-ICP-15.
Resolução nº 72	Aprova a versão 4.0 dos critérios e procedimentos para realização de auditorias nas entidades da ICP-BRASIL.
Retificação da Resolução nº 72	
Resolução nº 73	Aprova a versão 2.0 dos termos de titularidade de incapazes, pessoa física e pessoa jurídica na ICP-Brasil.

AGIPRO

Principais Documentos da ICP-Brasil

Resoluções

Resolução	Descrição
Resolução nº 74	Aprova a versão 3.2 DOC-ICP-05, versão 4.3 DOC-ICP-03 e versão 1.3 do DOC-ICP-03.01.
Resolução nº 75	Aprova a versão 3.3 do documento de requisitos mínimo para as declarações de práticas de certificação das autoridades certificadoras da icp-Brasil(DOC-ICP-05).
Resolução nº 76	Aprova a versão 2.0 do documento visão geral sobre as assinaturas digitais na ICP-Brasil (DOC-ICP-15).
Resolução nº 77	Aprova a versão 3.1 do documento requisitos mínimos para as políticas de certificado na ICP-Brasil (DOC-ICP-04).
Resolução nº 78	Aprova a versão 1.2 do documento de visão geral do sistema de carimbos do tempo na ICP-Brasil (DOC-ICP-11).
Resolução nº 79	Aprova a versão 3.4 do documento requisitos mínimos para as declarações de práticas de certificação das autoridades certificadoras da ICP-Brasil.(DOC-ICP-05).
Resolução nº 81	Aprova a versão 4.1 do documento declaração de práticas de certificação da autoridade certificadora raiz da ICP-Brasil (DOC-ICP-01).
Resolução nº 82	Aprova a versão 1.0 do documento manual de uso da marca da ICP-BRASIL, e a gestão de conteúdo do sítio da infraestrutura de chaves públicas brasileira (ICP-BRASIL).
Resolução nº 83	Aprova a versão 4.4 do documento critérios e procedimentos para credenciamento das entidades integrantes da ICP-Brasil (DOC-ICP-03).
Resolução nº 84	Aprova a versão 3.2 do DOC-ICP4 e a versão 3.5 do DOC-ICP-05 cujas alterações se referem aos procedimentos para a emissão de certificados digitais que integram o documento de registro de identidade civil – RIC.
Retificação da Resolução nº 84	
Resolução nº 85	Estabelece condição transitória para o requisito de obrigatoriedade de homologação ICP-BRASIL para equipamentos de Certificação Digital.
Resolução nº 86	Aprova a versão 4.5 do documento critérios e procedimentos para credenciamento das entidades integrantes da ICP-BRASIL (DOC-ICP-03).

Principais Documentos da ICP-Brasil

Resoluções

Resolução	Descrição
Resolução nº 87	Aprova a versão 4.0 do documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL (DOC-ICP-04).
Resolução nº 88	Aprova a versão 4.6 do documento critérios e procedimentos para credenciamento das entidades integrantes da ICP-BRASIL (DOC-ICP-03).
Resolução nº 89	Estabelece condição transitória para o requisito de obrigatoriedade de homologação ICP-BRASIL para equipamentos de certificação digital.
Resolução nº 90	Aprova a versão 3.6 do DOC-ICP-05 e a versão 1.6 do DOC-ICP-03.01.
Resolução nº 91	Aprova a versão 5.0 do documento requisitos mínimos para as políticas de certificado na ICP-BRASIL (DOC-ICP-04).
Resolução nº 92	Aprova a versão 2.1 do documento visão geral sobre assinaturas digitais na ICP-BRASIL (DOC-ICP-15).
Resolução nº 93	Estabelece o documento visão geral sobre Certificado de Atributo versão 1.0 para a ICP-Brasil(DOC-ICP-16).
Resolução nº 94	Aprova a versão 4.2 do documento declaração de práticas de certificação da autoridade certificadora raiz da icp-brasil(DOC-ICP-01).
Resolução nº 95	Aprova a versão 5.1 do documento requisitos mínimos para as políticas de certificado na icp-brasil (DOC-ICP-04).
Resolução nº 96	Aprova a versão 3.0 do documento regulamento para homologação de sistemas e equipamentos de certificação digital no âmbito da icp-brasil (DOC-ICP-10).
Resolução nº 97	Autoriza procedimento específico para atendimento à emissão de passaportes brasileiros.

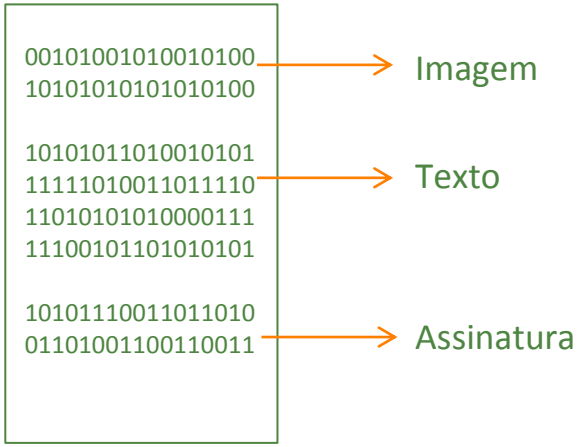
DOCUMENTO ELETRÔNICO CONFIÁVEL

- O que é o documento eletrônico.
- Vantagens e desvantagens do documento eletrônico.
- Problemas do documento eletrônico.
  - Credibilidade do papel x eletrônico
    - Assinatura manuscrita x Assinatura digital
  - Barreira cultural : selo, assinatura, carimbo.
  - Barreira tecnológica: uso x conhecimento.
- O documento eletrônico confiável

Conceitos de Documento

O documento

O documento eletrônico



Vantagens do documento Eletrônico

- Rapidez na elaboração
- Rapidez na transmissão
- Alta capacidade de armazenamento
- Facilidade de criar cópias
- Redução de custo com armazenamento
- Redução de custo com impressão
- Resistência ao envelhecimento, deterioração

Desvantagens do documento Eletrônico

- Facilidade de criar cópias
- Vulnerabilidade de sistemas
- Velocidade da evolução tecnológica com alteração constante de padrões
- Credibilidade cultural do papel
  - Recibo, Carimbo, Protocolo, etc..
- Falta de conhecimento da legislação

AGIPRO

Problemas do Documento Eletrônico

Credibilidade: Papel x Eletrônico

– Como garantir os requisitos de segurança do documento?

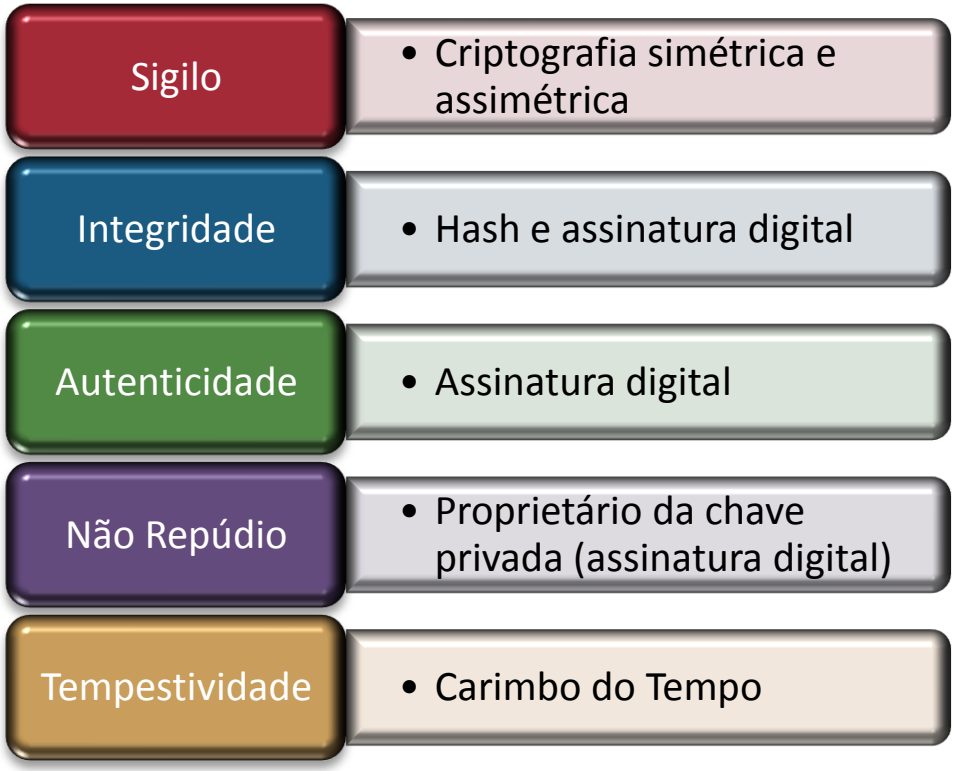
- Autenticidade
- Integridade
- Não-Repúdio
- Sigilo
- Tempestividade

– Barreira Cultural

  – A assinatura digital é visível no documento?
  – E os selos e carimbos?

– Barreira Tecnológica

  – É seguro usar a assinatura digital?
  – E se roubarem minha senha?
  – O que fazer se eu perder meu certificado?
  – O documento eletrônico tem validade jurídica?

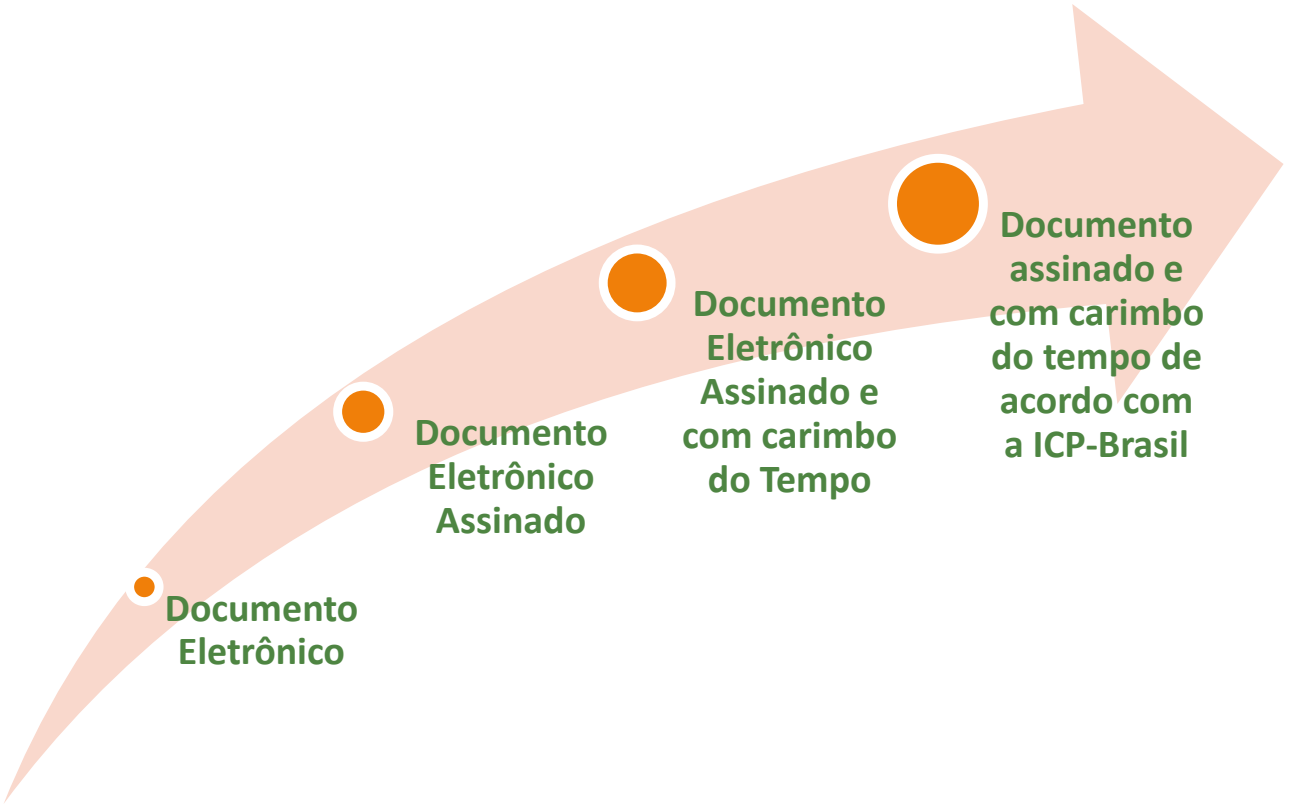


Características indispensáveis

– É aquele que atende aos requisitos de segurança exigidos.

– É aquele que atende a legislação vigente aplicável.

– O custo de quebra dos requisitos do documento é maior que o valor do documento.



- **Confiança**
- **Segurança**
- **Valor Jurídico**

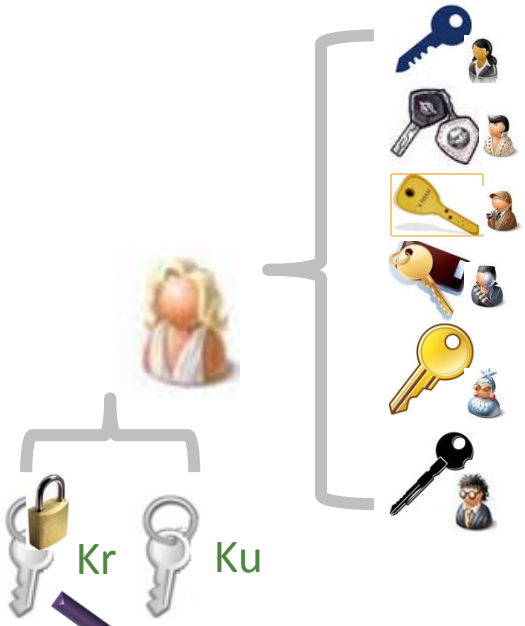
ASSINATURA DIGITAL

- O que é assinatura digital
  - Assinando e verificando a assinatura (o mais crítico é validar o certificado digital)
- Padrões de assinatura digital ICP-BRASIL
  - AD-RB
  - AD-RT
  - AD-RV
  - AD-RC
  - AD-RA

Assinando e verificando a assinatura digital

– Alice deseja enviar uma mensagem assinada para bob.

– Quais chaves deverão ser utilizadas para cifrar e decifrar a mensagem?



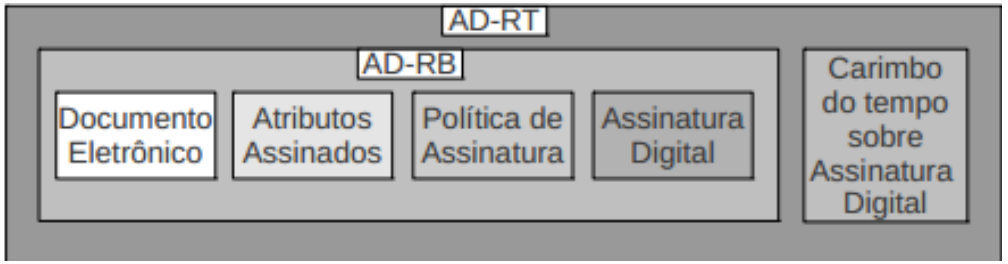
Formato Geral

```
SignedData ::= SEQUENCE {
        version CMSVersion,
        digestAlgorithms DigestAlgorithmIdentifiers,
        encapContentInfo EncapsulatedContentInfo,
        certificates [0] IMPLICIT CertificateSet OPTIONAL,
        crls [1] IMPLICIT RevocationInfoChoices OPTIONAL,
        signerInfos SignerInfos }

DigestAlgorithmIdentifiers ::= SET OF DigestAlgorithmIdentifier

SignerInfos ::= SET OF SignerInfo

EncapsulatedContentInfo ::= SEQUENCE {
        eContentType ContentType,
        eContent [0] EXPLICIT OCTET STRING OPTIONAL }

SignerInfo ::= SEQUENCE {
        version CMSVersion,
        sid SignerIdentifier,
        digestAlgorithm DigestAlgorithmIdentifier,
        signedAttrs [0] IMPLICIT SignedAttributes OPTIONAL,
        signatureAlgorithm SignatureAlgorithmIdentifier,
        signature SignatureValue,
        unsignedAttrs [1] IMPLICIT UnsignedAttributes
OPTIONAL }
```

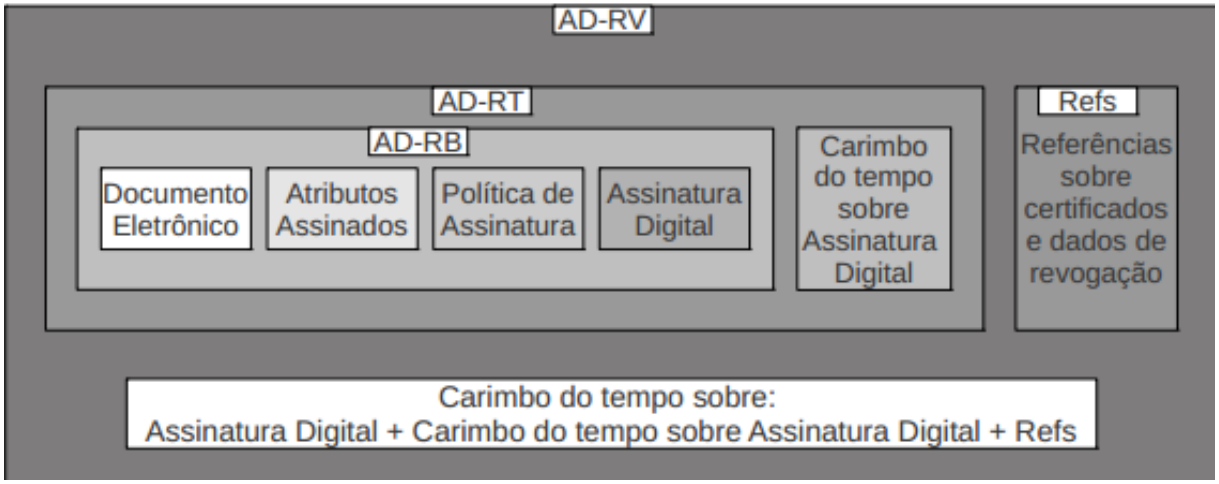
Assinatura Digital

AD-RB

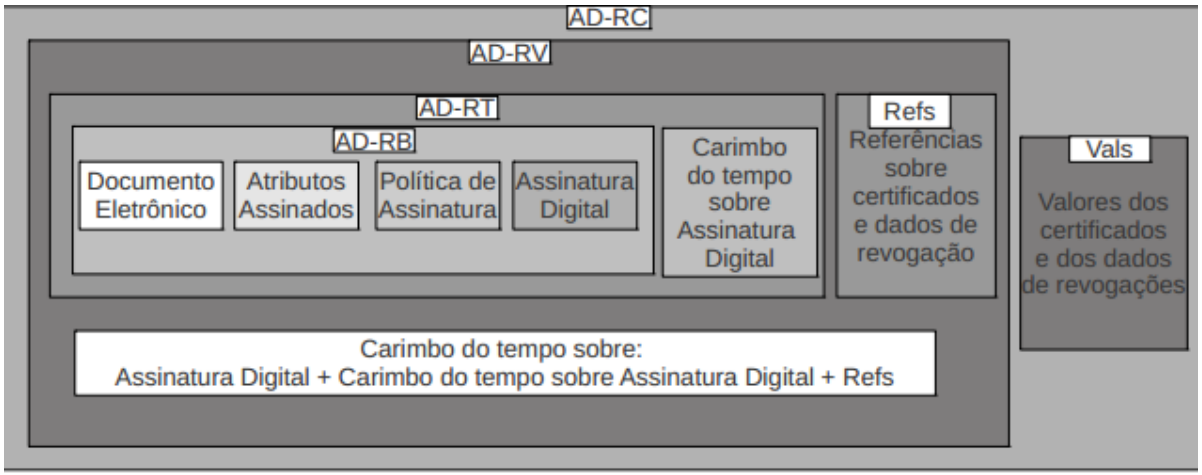
AD-RT



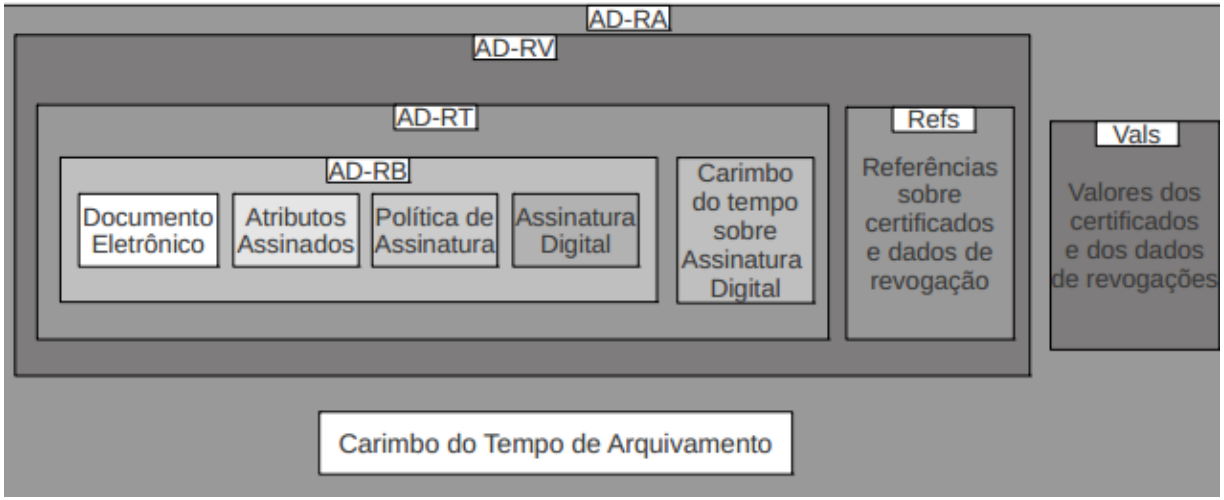
AD-RV



AD-RC

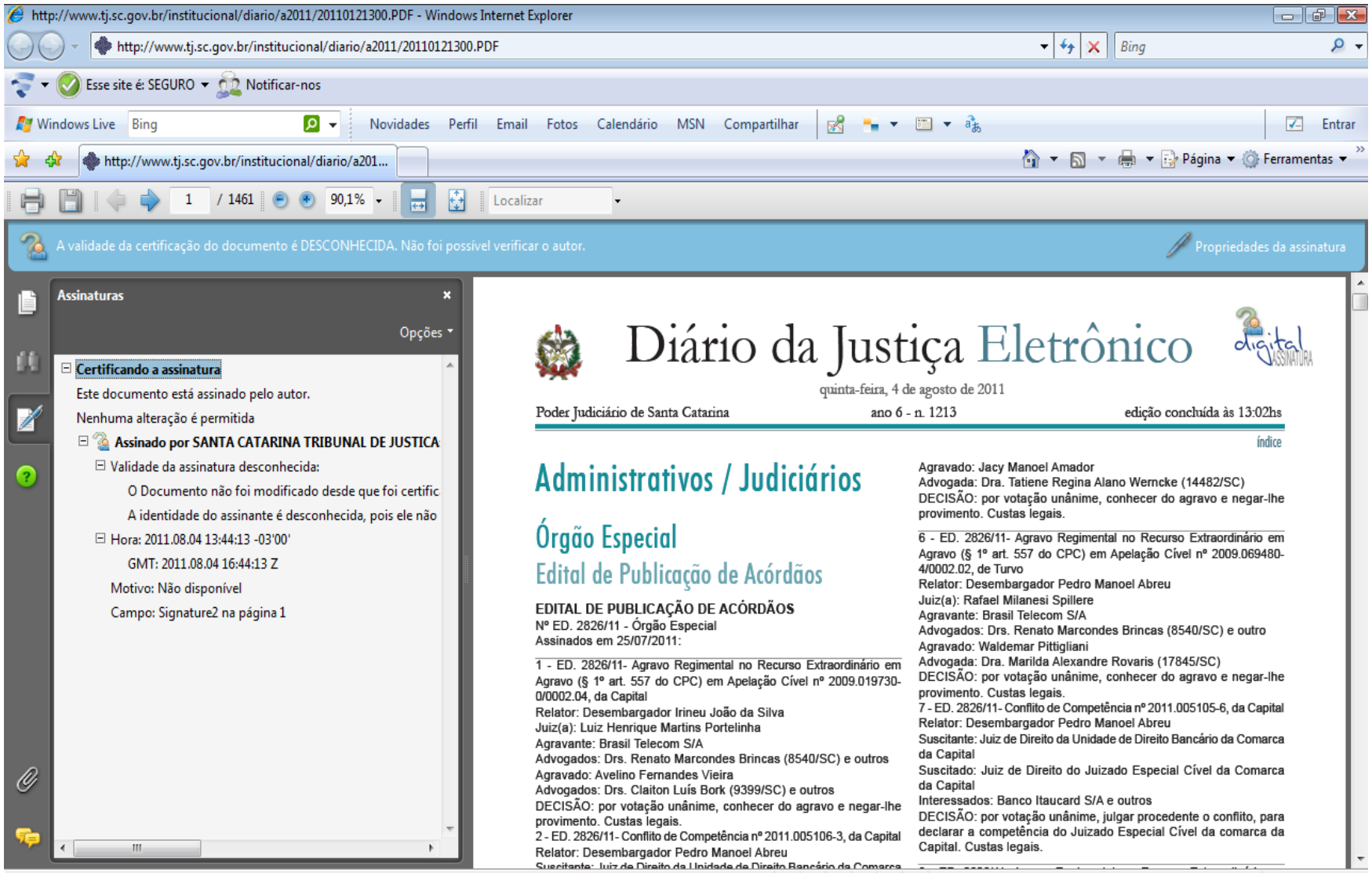

AD-RC
AD-RV
AD-RT
AD-RB
Documento Eletrônico
Atributos Assinados
Política de Assinatura
Assinatura Digital
Carimbo do tempo sobre Assinatura Digital
Refs
Referências sobre certificados e dados de revogação
Vals
Valores dos certificados e dos dados de revogações
Carimbo do tempo sobre:
Assinatura Digital + Carimbo do tempo sobre Assinatura Digital + Refs

AD-RA


AD-RA
AD-RV
AD-RT
AD-RB
Documento Eletrônico
Atributos Assinados
Política de Assinatura
Assinatura Digital
Carimbo do tempo sobre Assinatura Digital
Refs
Referências sobre certificados e dados de revogação
Vals
Valores dos certificados e dos dados de revogações
Carimbo do Tempo de Arquivamento

ASSINATURA DIGITAL

Exemplo de Assinatura Digital em um documento PDF



CARIMBO DO TEMPO

- O que é o Carimbo do Tempo
- A Autoridade de Carimbo do Tempo

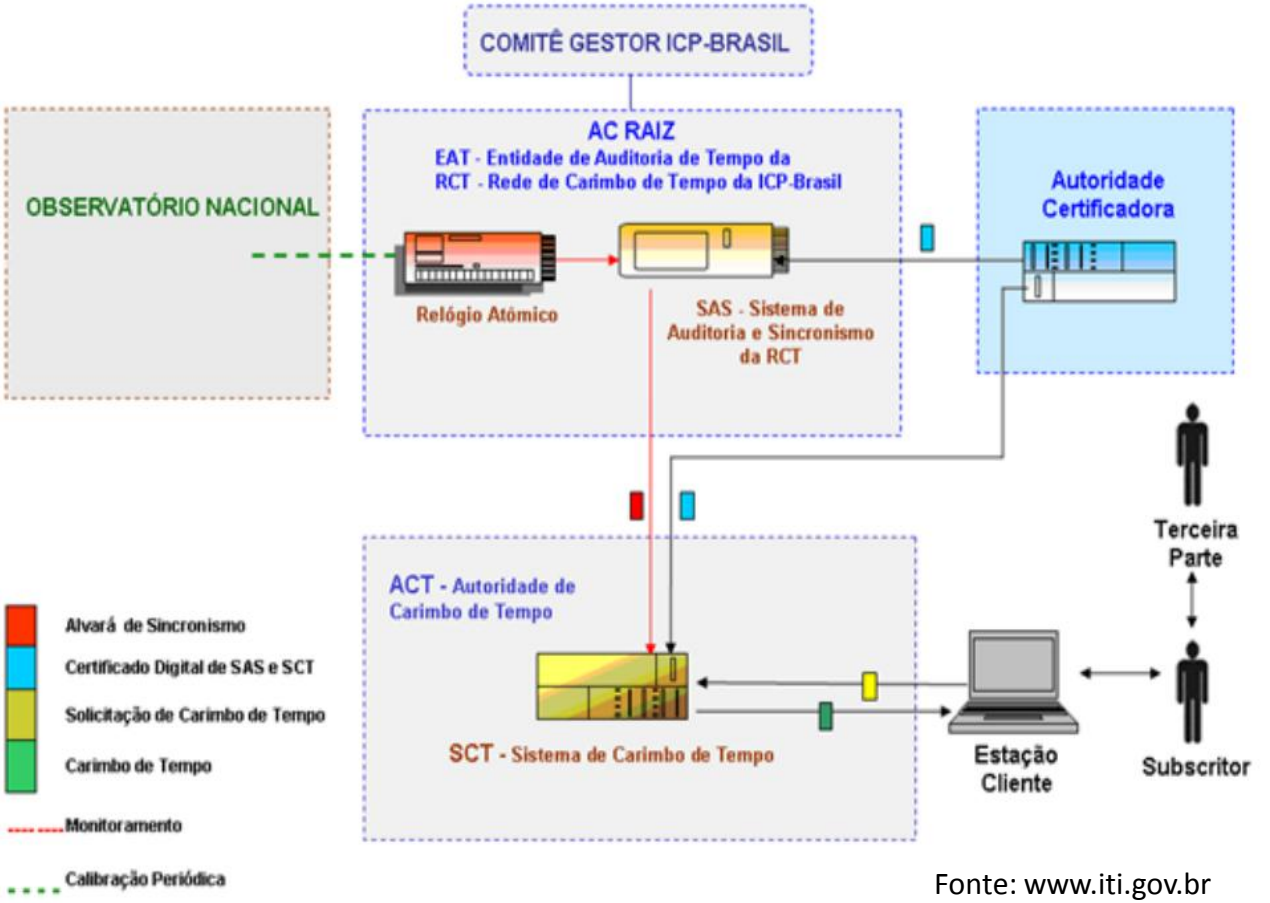
CARIMBO DO TEMPO

O que é o Carimbo do Tempo?

– Documento eletrônico que serve como evidência de que uma informação digital existia numa determinada data e hora passada.

Fonte: www.iti.gov.br

A Autoridade de Carimbo do Tempo na ICP-Brasil



Fonte: www.iti.gov.br

DÚVIDAS?????

MUITO OBRIGADO!!

Sérgio Roberto de Lima e Silva Filho

Consultor

Agipro Sistemas Computacionais e Consultoria Ltda.