CELEPAR INFORMÁTICA do PARANÁ

Tecnologia para a Democracia

PLATAFORMA DE DESENVOLVIMENTO

TUTORIAL BÁSICO SOBRE CERTIFICAÇÃO DIGITAL

http://www.frameworkpinhao.pr.gov.br/

TUTORIAL SOBRE CERTIFICAÇÃO DIGITAL

Tópicos que serão abordados:

- PARA QUÊ UTILIZAR
- ASPECTOS TEÓRICOS
- ASPECTOS JURÍDICOS
- ASPECTOS CULTURAIS
- CONCEITOS RELACIONADOS
- USOS
- SOLUÇÕES / FERRAMENTAS
- TEMPESTIVIDADE DIGITAL

- PARA QUÊ UTILIZAR

A Certificação Digital é requerida ou recomendada quando se deseja atender, pelo menos, um dos seguintes requisitos:

- **Aumentar o nível de Segurança em:**
  - ✓ Serviços de autenticação de agentes
  - ✓ Protocolos de comunicação
  - ✓ Servidores e Aplicações (https/TSL)
  - ✓ Sigilo de informações (Criptografia)

- ...cont PARA QUÊ UTILIZAR

- **Garantia de Autenticidade e Integridade:**
  - ✓ Através de Assinatura Digital
  - ✓ Para qualquer tipo de documento digital
  - ✓ Mensagens eletrônicas (e-mail)
  - ✓ Procedimentos/Processos eletrônicos confiáveis
  - ✓ Evitar fraudes digitais.

- **Obter Garantias e Suportes Legais:**
  - ✓ Eficácia Probatória
  - ✓ Não repúdio

- ...cont PARA QUÊ UTILIZAR

- **Outros Benefícios:**
  - ✓ Melhorar a confiabilidade no ambiente Digital.
  - ✓ Diminuição do uso de papel.
  - ✓ Agilidade e diminuição dos custos dos serviços públicos.

ASPECTOS TEÓRICOS

- **Conceito de Agente**

Entende-se por Agente, qualquer entidade que pode interagir, de alguma forma, com qualquer outra no mundo (ambiente) digital. ex.: pessoas, sistemas, web-sites, etc...

- **Conceito de Certificado Digital**

O Certificado Digital é um arquivo em formato eletrônico que contém um conjunto de **informações (nome, e-mail, cpf, url, ...)** que identificam de forma única um **agente.**

ASPECTOS TEÓRICOS

- **Criptografia**

São técnicas utilizadas para manter o segredo de informações, impedindo que as mesmas possam ser lidas por aqueles que não estariam autorizados a conhecê-las.

No mundo digital a técnica mais eficiente é feita através de cifras e algorítimos baseados nos conceitos de **chaves criptográficas**.

- **Chaves Criptográficas**

São códigos computacionais gerados através de fórmulas matemáticas que servem como base para gerar a criptografia pelos certificados digitais. A criptografia é também uma das técnicas utilizadas para gerar a Assinatura Digital. Estas chaves também farão parte do **Certificado Digital**.

Nos certificados digitais a técnica utilizada é a do sistema de chaves públicas baseada no conceito de **criptografia assimétrica**.

cont...

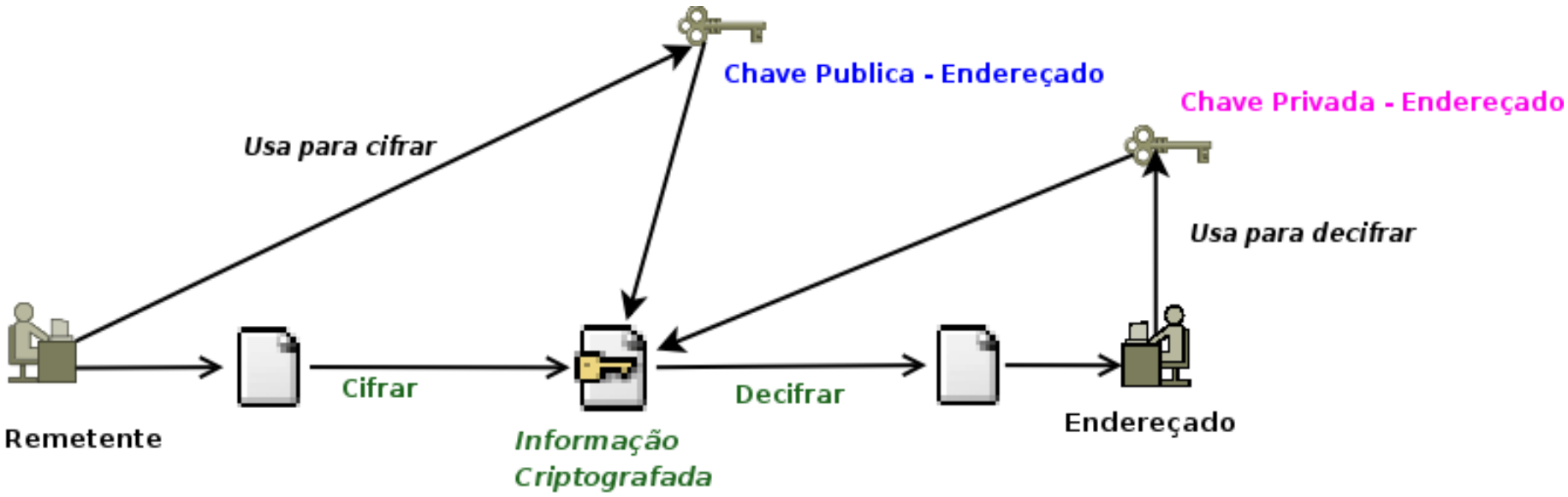
ASPECTS TEÓRICOS

...cont

Esta técnica utiliza um par de chaves criptográficas sendo uma de conhecimento PRIVADO e outra de conhecimento PÚBLICO. Surgindo assim o termo chave PÚBLICA e chave PRIVADA.

As fórmulas matemáticas utilizadas garantem que somente a chave correspondente de cada par é capaz de desfazer a criptografia gerada pela outra, e estas fórmulas também garantem a unicidade de cada chave. Hoje é computacionalmente improvável a dedução de uma pela outra.

ASPECTOS TEÓRICOS



Exemplo de Criptografia Assimétrica

Ex: - RSA (mais eficiente)

- DSA (governo EUA).

ASPECTOS TEÓRICOS

- **Arquivo/Documento Digital**

Qualquer conjunto de dados digitais (bits/bytes) que representam alguma informação do mundo real (analógico). Ex: textos, imagens, estruturas de dados, vídeos, áudios, etc.

Podem ser originalmente eletrônico ou convertido do analógico (digitalização/cópia).

- **Hash (resumo)**

- Um hash ou resumo é uma seqüência de letras e/ou números gerada por algoritmos de dispersão e possui tamanho único em bits para qualquer arquivo.

- Essa seqüência busca identificar um arquivo ou documento digital de forma única e inequívoca. É um método para transformar dados de tal forma que o resultado seja probabilisticamente exclusivo. Além disso, as funções usadas garantem que não é possível a partir de um valor de hash retornar à informação original.

cont...

ASPECTOS TEÓRICOS

cont...

Devem garantir baixíssima colisão (mesmo hash para arquivos diferentes)

Mais conhecidos:

- MD4: 1990/91 por Ron Rivest,
- MD5: (Message-Digest Algorithm 5) RSA Data Security, Inc.,
- SHA-1 (Secure Hash Algorithm): Desenvolvido pelo NIST e NSA.

ASPECTOS TEÓRICOS

- **Assinatura Digital**

É um conjunto de informações, criptografadas, contendo os dados referentes ao conteúdo dos documentos/arquivos que foram assinados.

Este conjunto é formado pelo conteúdo gerado através de técnicas de Hash (resumo), ou seja, a identificação única de cada arquivo digital, que na seqüência é criptografado com a chave **Privada** do Certificado do **assinante**. Conseqüentemente, a assinatura será validada com a chave **Pública** do Certificado do **assinante**.

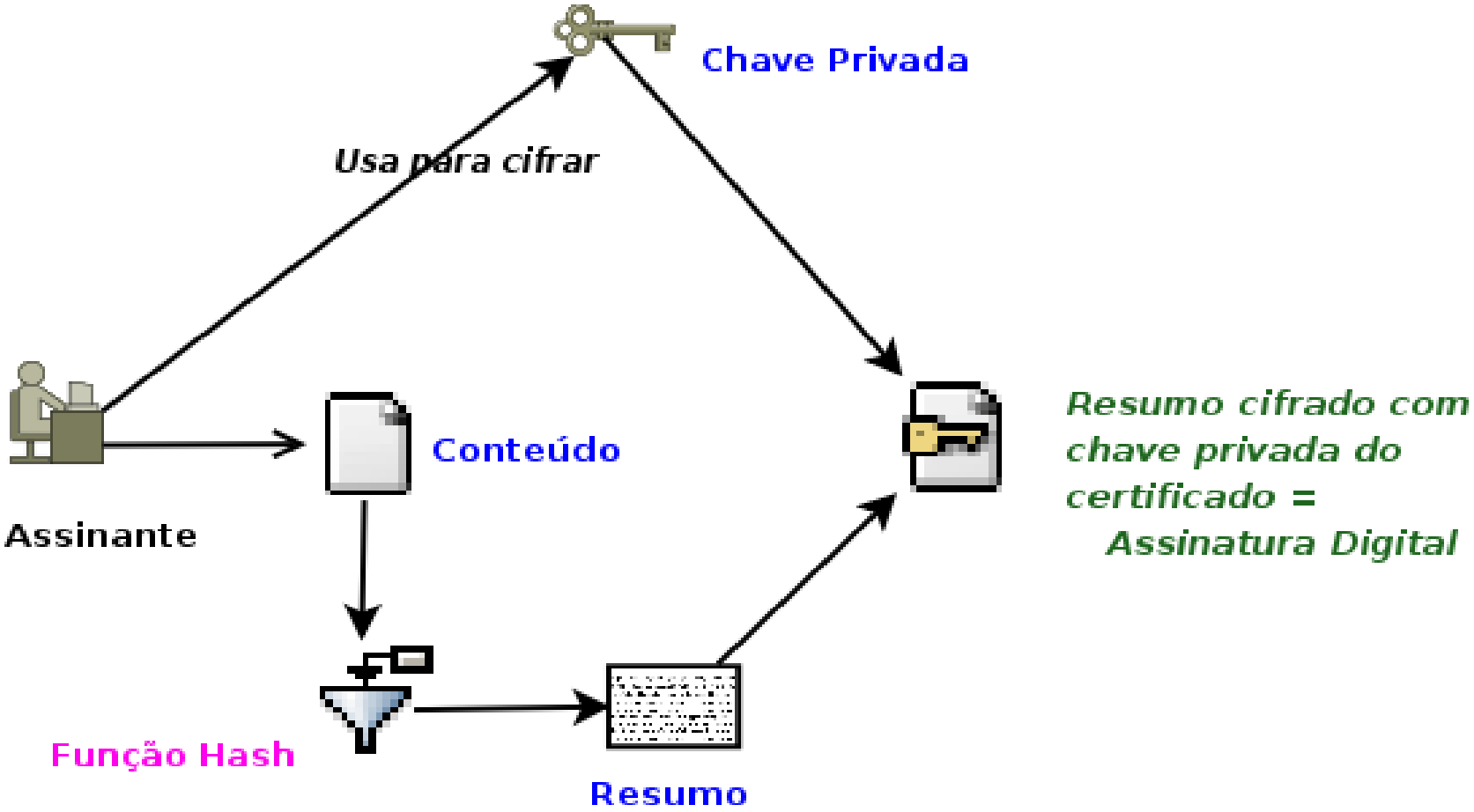
cont..

ASPECTOS TEÓRICOS

...cont

É esse arquivo, ou seja a Assinatura Digital gerada, com um certificado **válido** e reconhecido, que garante a **autenticidade** e **integridade** da informação através de uma conexão lógica com o conteúdo assinado.

ASPECTS TEÓRICOS



Exemplo de geração de assinatura

- **Validação de Assinatura Digital**

A validação de uma assinatura digital é feita através da execução do procedimento **inverso** ao da geração da Assinatura Digital. De posse do arquivo, considerado original, e o arquivo da Assinatura Digital, utiliza-se a chave **Pública** do Certificado do Assinante para de-criptografar e recuperar o resumo e compará-lo com o conteúdo (que será o resumo gerado no momento da comparação) do arquivo que se quer validar. Sabendo-se que somente uma **única** chave **Pública** corresponde a outra única chave Privada, tem-se a certeza da identificação do Assinante.

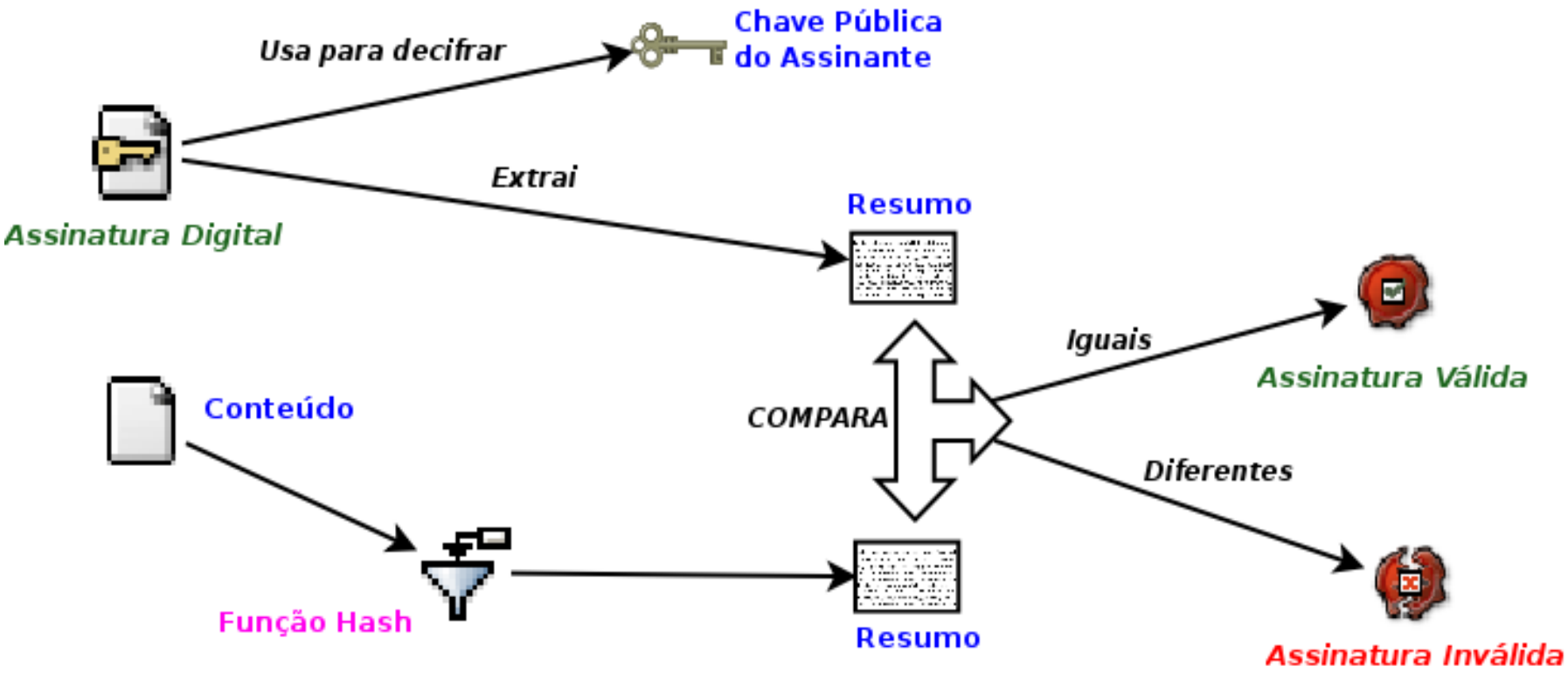
..cont.

- **Validação de Assinatura Digital**

..cont.

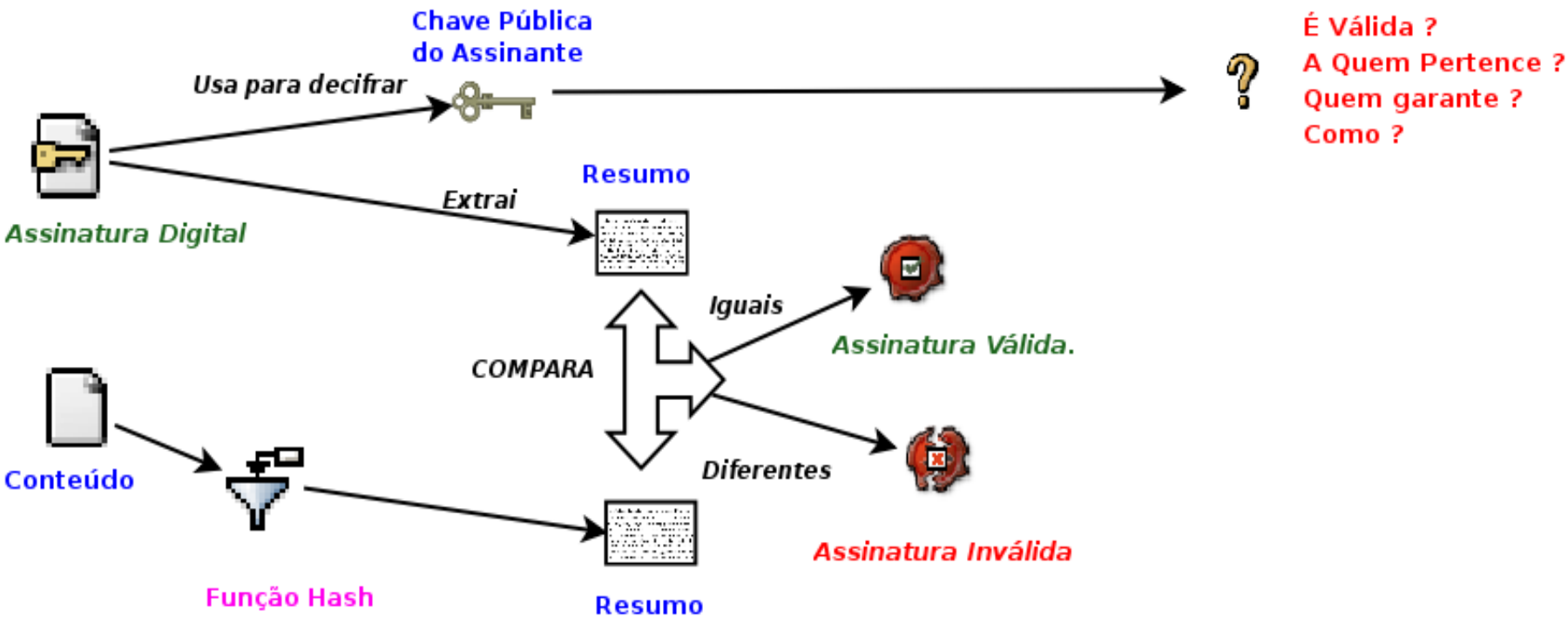
Se a comparação dos Resumos (hash) não for positiva, significa que a assinatura não corresponde ao arquivo apresentado, ou que o mesmo, ou a própria assinatura, foram alterados ou corrompidos de alguma maneira. Também é impossível a utilização de outra chave pública que não seja correspondente à chave privada que foi usada na geração da assinatura.

ASPECTOS TEÓRICOS



Exemplo de validação de Assinatura Digital

ASPECTOS TEÓRICOS



Exemplo de validação de Assinatura Digital

ASPECTOS TEÓRICOS

- **<u>Conceito de Certificação Digital</u>**

A Certificação Digital é todo um conjunto de **técnicas, processos e normas** estabelecidas ou adotadas**,** que visam propiciar mais segurança às comunicações e transações eletrônicas, e permite também a garantia de **Autenticidade e Integridade** dos documentos e procedimentos eletrônicos.

cont...

ASPECTOS TEÓRICOS

...cont

A Certificação digital aplica, principalmente, os conceitos de **Criptografia e Assinatura Digital**.

A sua implantação depende do uso de certificados digitais com o respectivo par de chaves criptográficas, sendo que a **validade e autenticidade** dos certificados devem ser **garantidas** por uma infra-estrutura de chaves públicas (**ICP**).

ASPECTOS TEÓRICOS

- **<u>Infra-estrutura de Chaves Públicas (ICP).</u>**

Uma ICP é todo o conjunto das soluções que dá sustentação às técnicas e processos para implantação da Certificação Digital.

A principal finalidade de uma ICP é garantir a legitimidade e autenticidade das informações contidas em um certificado.

Para esta finalidade uma ICP adota/define um conjunto de normas e padrões que são as políticas da ICP.

Os principais componentes de uma ICP são:

Autoridade Certificadora (AC) e

Autoridade de Registro (AR)

ASPECTOS TEÓRICOS

- **Autoridade Certificadora (AC)**

É a entidade responsável por garantir a autenticidade e validade de certificados digitais. Para isto a AC possui também um par de chaves que é utilizado para assinar os certificados garantidos por ela. É através da validação da assinatura da AC que é possível verificar a autenticidade de um certificado. Uma AC pode inclusive assinar os certificados de AC's de nível inferior (Sub-AC).

São algumas das principais responsabilidades da AC:

- Publicar/determinar todas as normas, políticas e padrões para o funcionamento da ICP.
- A guarda segura e inviolabilidade de sua chave privada.
- Gerenciar o ciclo de vida do Certificado.

ASPECTOS TEÓRICOS

- **Autoridade de Registro (AR)**

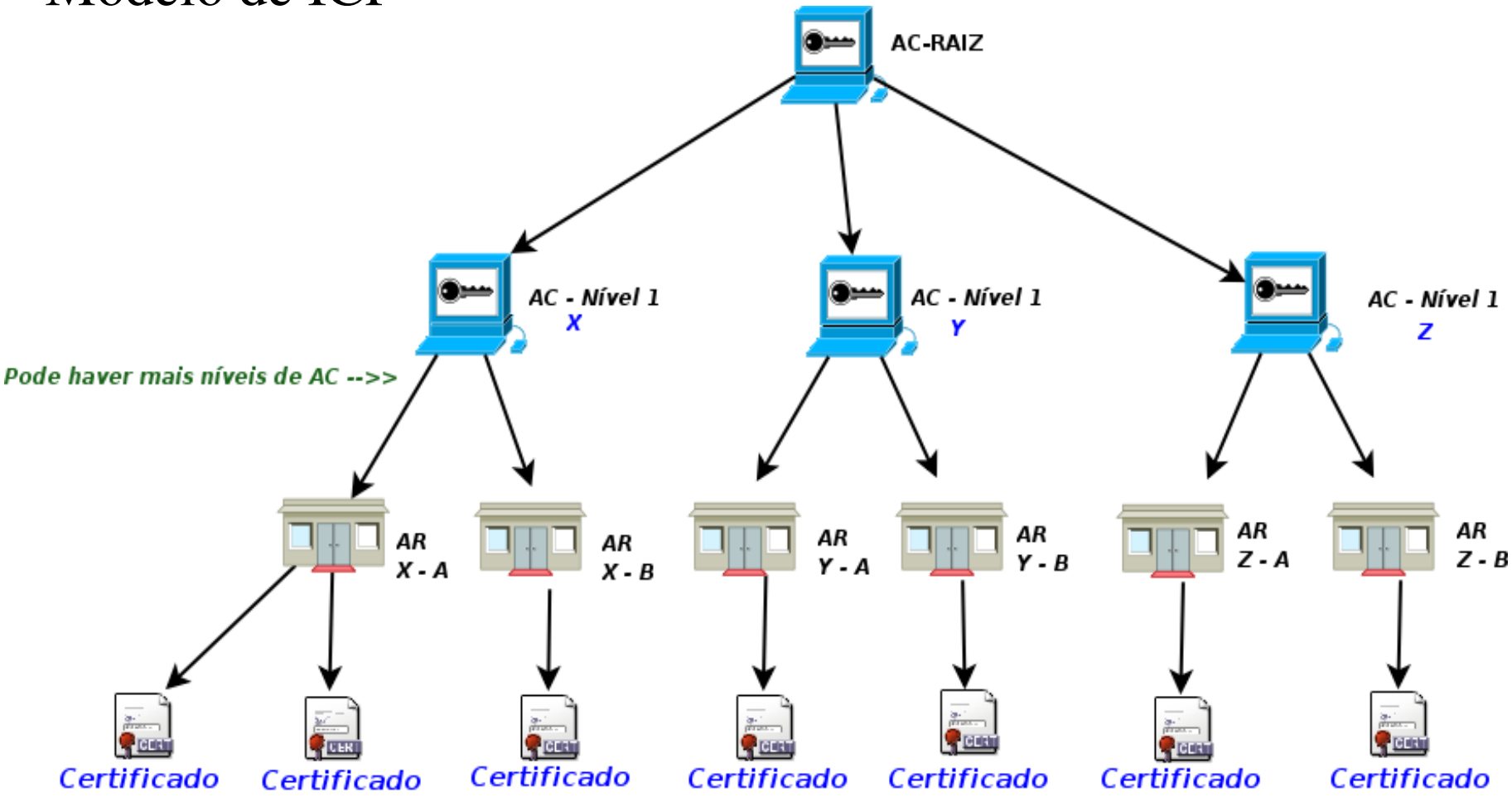
É a entidade responsável pela coleta e validação dos dados dos agentes que irão gerar e usar os certificados digitais. É também responsabilidade desta entidade a guarda dos documentos necessários para a verificação da legitimidade e identidade do agente.

Deverá obrigatoriamente estar credenciada junto a uma AC, pois será a AR que representará a AC perante um agente.

É o escritório de representação de uma AC.

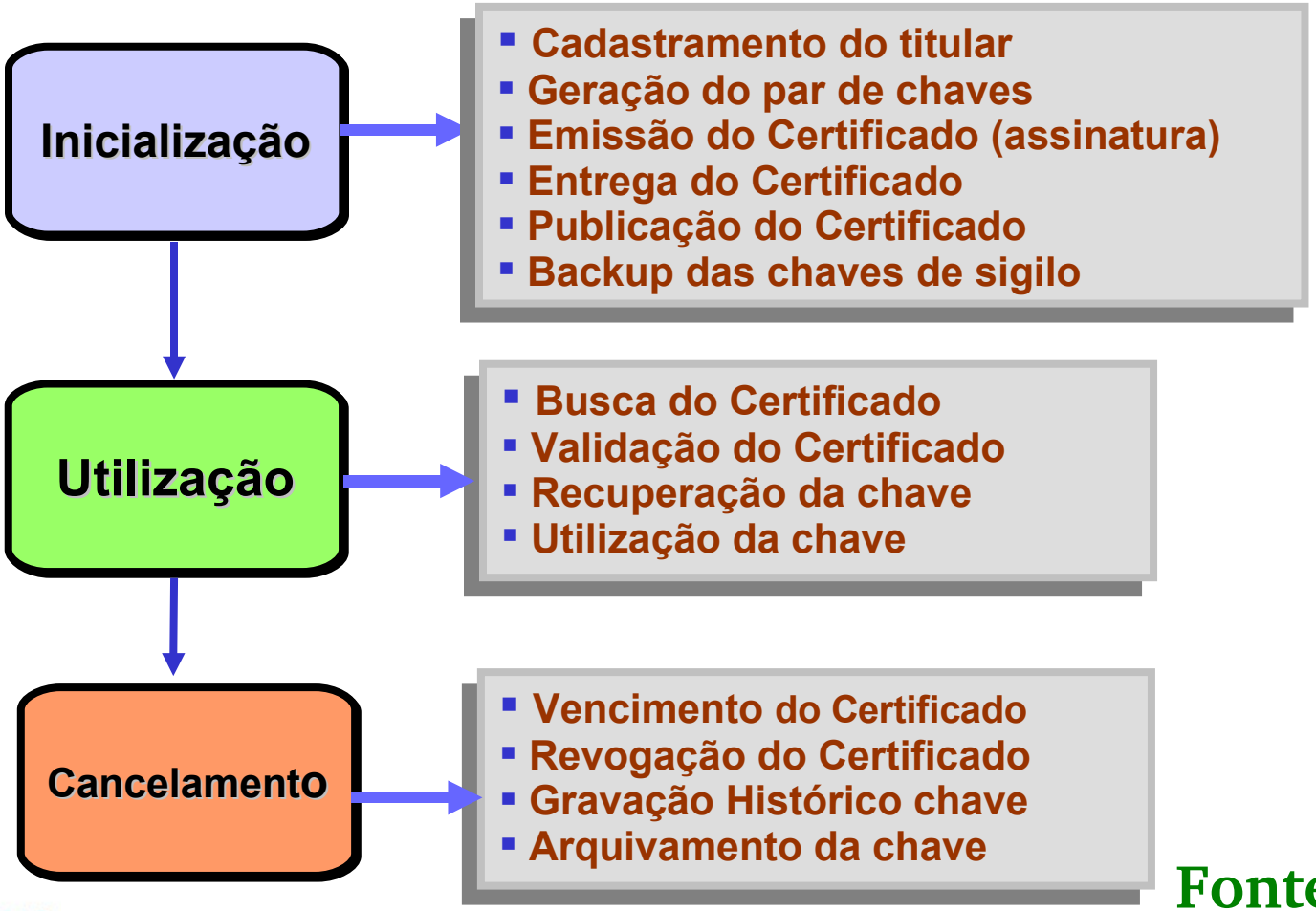
ASPECTOS TEÓRICOS

Modelo de ICP



ASPECTOS TEÓRICOS

- **Ciclo de Vida do Certificado**



Fonte: USP

ASPECTOS JURÍDICOS

- **<u>Eficácia Probatória</u>**

Validade jurídica dos procedimentos probatórios, ou seja, nos critérios de identificação de adulteração no caso de falsidade documental, que são evidências que possam provar a falsidade no ambiente eletrônico.

ASPECTOS JURÍDICOS

- **Não Repúdio**

Não-Repúdio, ou não recusa, é o atributo legal que prevê a garantia de que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica (assinou um documento ou formulário eletrônico), não poderá posteriormente negar sua autoria.

- A instituição Brasileira que garante suporte legal a estes dois requisitos é a ICP-BRASIL.

ASPECTOS JURÍDICOS

- **ICP-BRASIL**

Criada a partir da Medida Provisória 2.200-2, de 24.10.2001, é um conjunto de AC's ordenadas em conformidade com as diretrizes e normas técnicas estabelecidas por um Comitê Gestor. **Somente** as transações realizadas com processo de certificação, envolvendo **certificados emitidos por autoridades credenciadas na ICP-Brasil,** presumem-se verdadeiras em relação aos signatários, dando **validade jurídica** aos documentos assinados digitalmente.

Fonte: ITI

ASPECTS JURÍDICOS

- **ICP-BRASIL** - CARACTERÍSTICAS

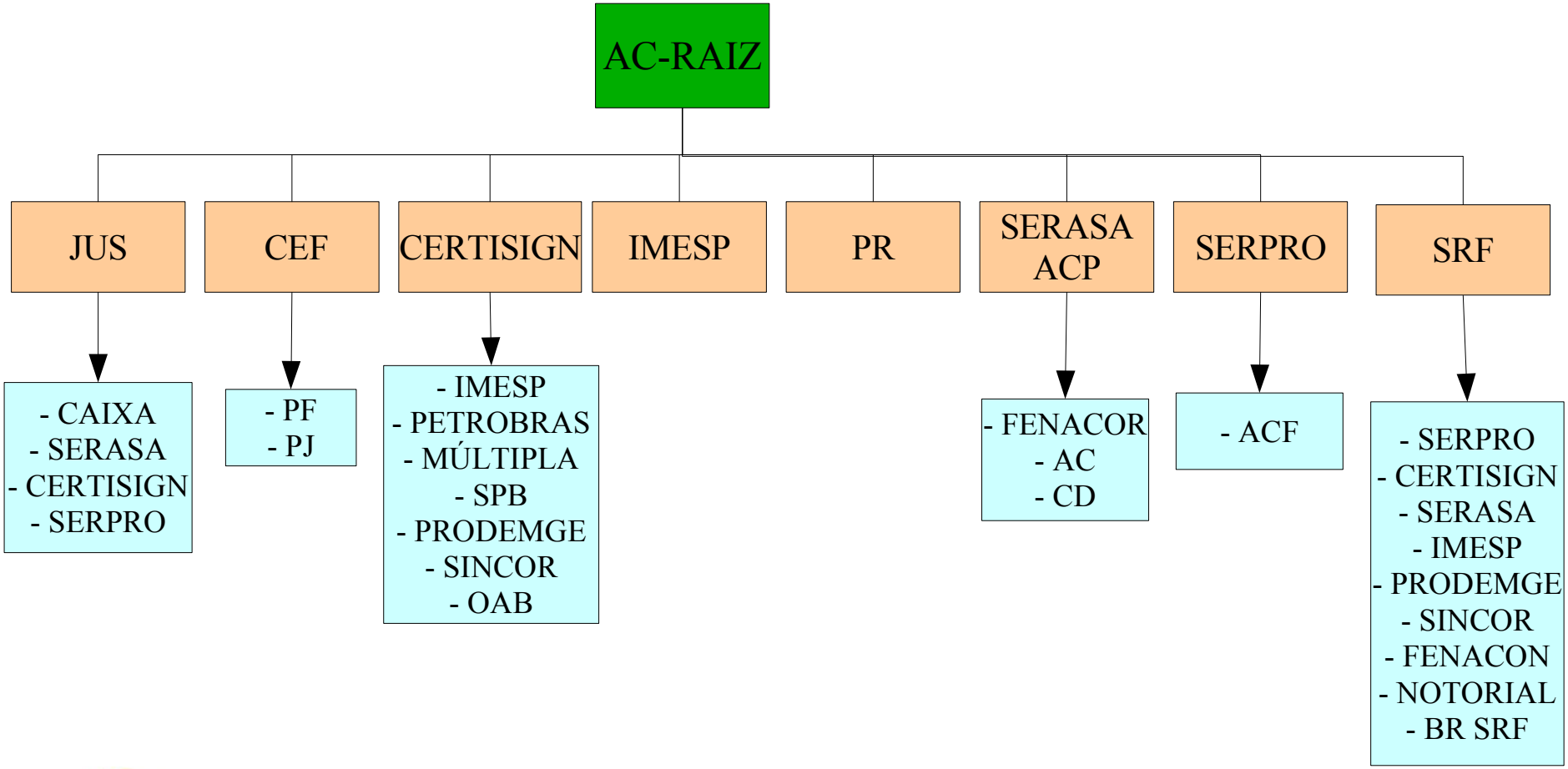
Uma das principais características da ICP-Brasil é sua estrutura hierárquica. No topo da estrutura, encontra-se a **Autoridade Certificadora Raiz** e, abaixo dela, estão as diversas entidades. O contrato de adesão é subordinado a um processo de credenciamento, no qual são analisadas a capacidade jurídica, econômico-financeira, fiscal e técnica de cada entidade. Também é exigida a contratação de seguro de responsabilidade civil e a realização de auditorias prévias e anuais.

A Entidade responsável no Brasil é o ITI (http://www.iti.gov.br/)

Fonte: ITI

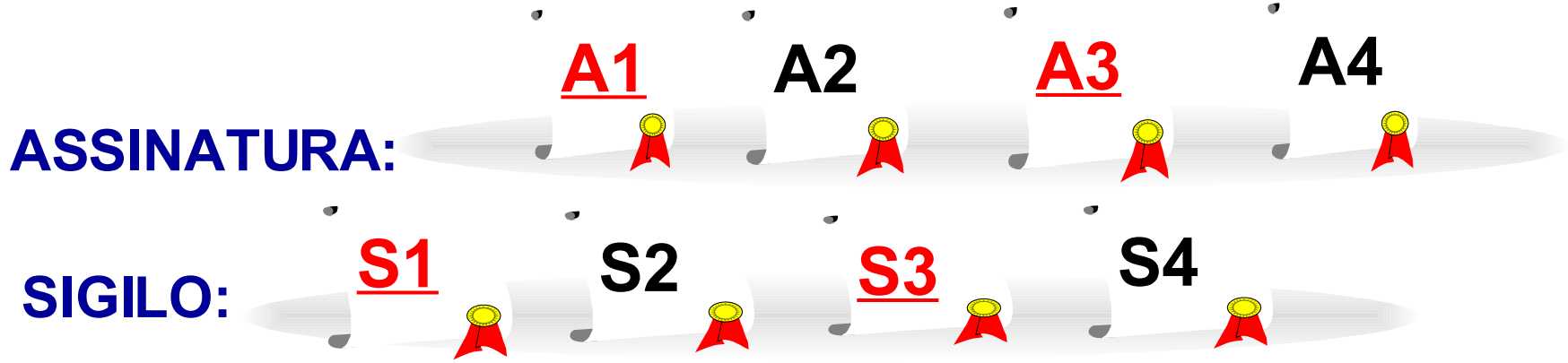
ASPECTOS JURÍDICOS

Estrutura da ICP-Brasil Atualizado: 10/07/2008



ASPECTOS JURÍDICOS

Tipos de Certificados ICP-Brasil



Nível de segurança - → +

- A1 e S1 Chave 1024 bits gerada por software para 1 ano
- A2 e S2 Chave 1024 bits gerada por hardware para 2 anos
- A3 e S3 Chave 1024 bits gerada por hardware para 3 anos
- A4 e S4 Chave 2048 bits gerada por hardware para 3 anos

ASPECTOS JURÍDICOS

Tipos de Certificados ICP-Brasil

- ***e-CPF, Identidade Digital, CertJUS, etc***: São nomes comerciais, geralmente são: A1 e A3(Token/SmartCard) e usados para identificar P**essoa Física**.

- ***e-CPF Simples*** é destinado exclusivamente ao responsável titular de Microempresa (ME) e Empresa de Pequeno Porte (EPP), optantes ou não do SIMPLES NACIONAL.

- Tecnicamente, todos tem o mesmo efeito prático.

ASPECTOS JURÍDICOS

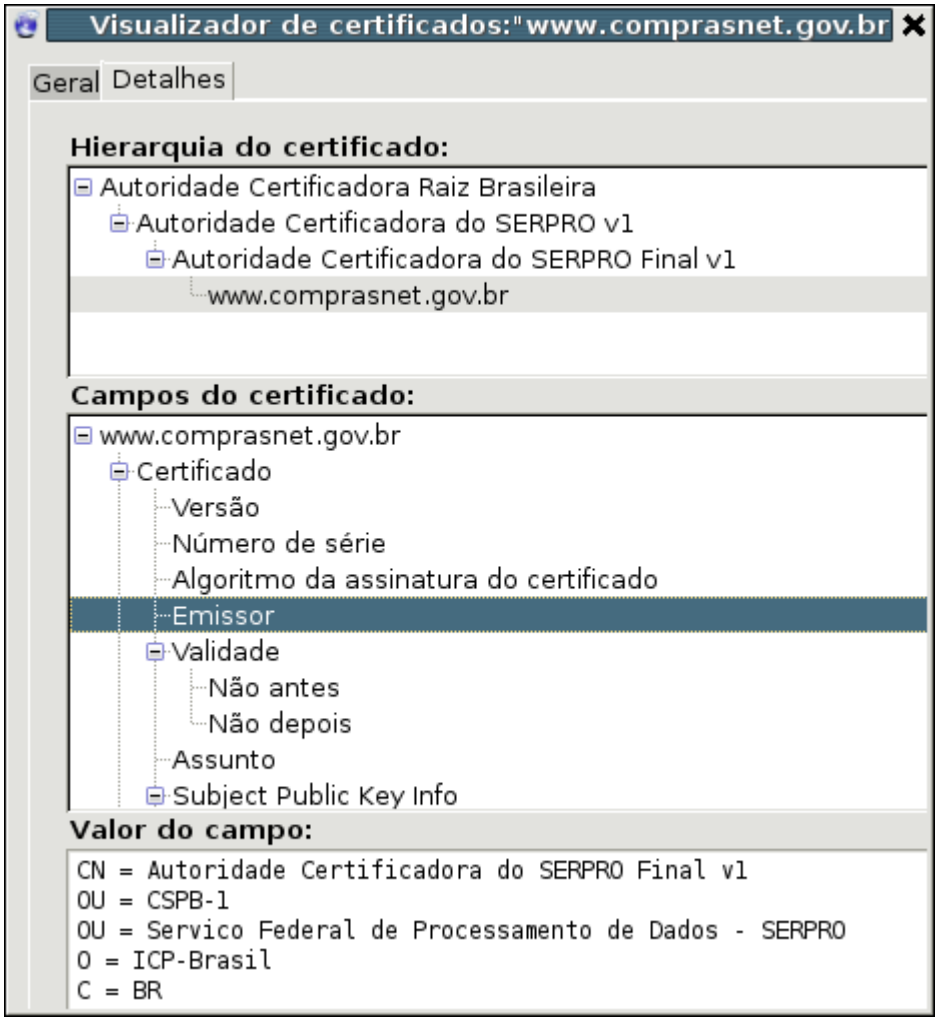
Tipos de Certificados ICP-Brasil

- ***e-CNPJ, CertJUS Empresarial, etc***: Também nomes comerciais, geralmente são: A1 e A3(Token/SmartCard) e usados para identificar P**essoa Jurídica**.

- ***Certificados de Servidor/Equipamento:*** São os certificados do tipo S1(mais comum), S2, S3, S4 (HSM), usados para identificar um Equipamento (IP, URL), ou uma Aplicação/Serviço (URL/Nome da Aplicação)

ASPECTOS JURÍDICOS

EXEMPLOS DE CERTIFICADOS VÁLIDOS:



ASPECTOS JURÍDICOS

LEI Nº 11.419, DE 19 DE DEZEMBRO DE 2006, que dispõe sobre a informatização do processo judicial; altera a Lei no 5.869, de 11 de janeiro de 1973-Código de Processo Civil; e dá outras providências.

"*Art. 11. Os* ***documentos produzidos eletronicamente*** *e juntados aos processos eletrônicos* ***com garantia da origem e de seu signatário****, na forma estabelecida nesta Lei,* ***serão considerados originais para todos os efeitos legais****.*"

ASPECTOS JURÍDICOS

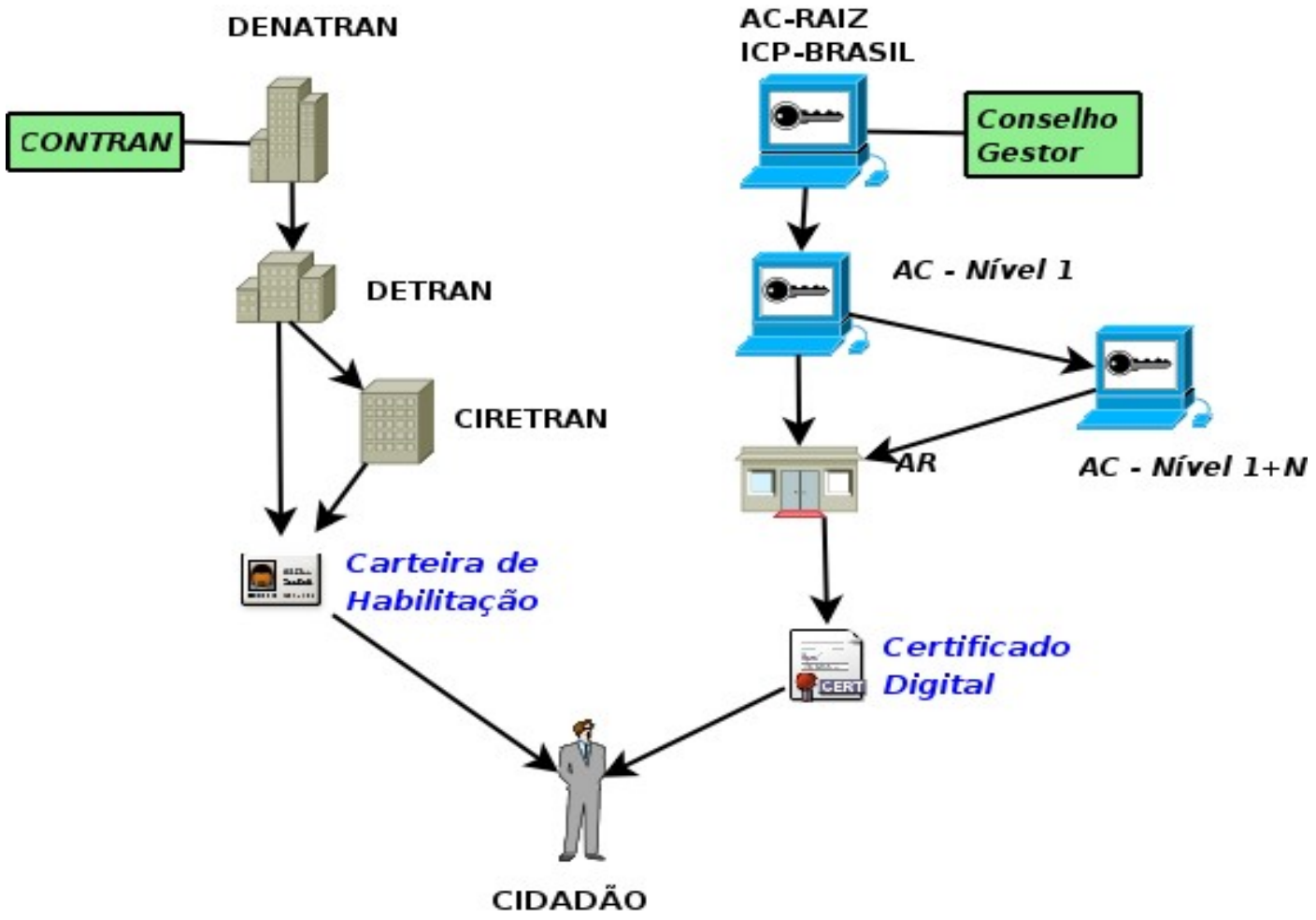
Provisória no. 2.200-2 de 24/08/2001:

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

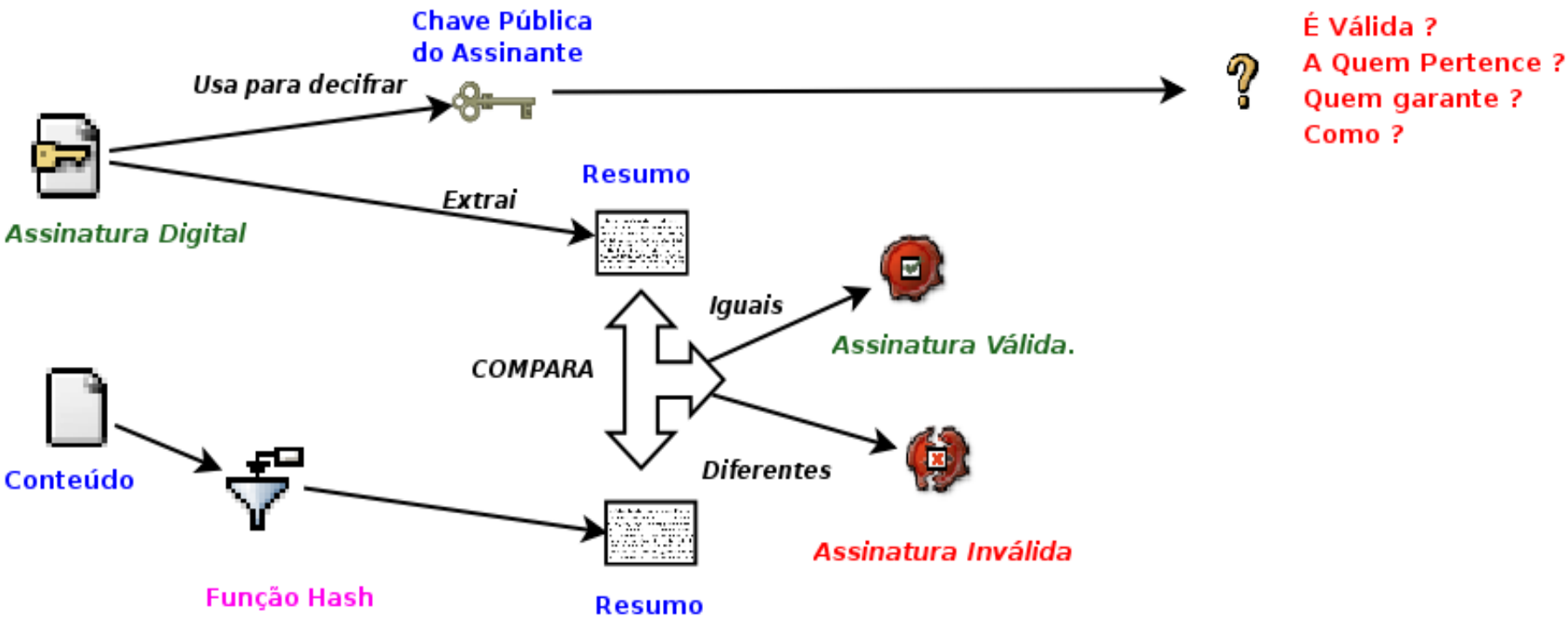
§ 1o As declarações constantes dos documentos em forma eletrônica, produzidos com a utilização de processo de ***certificação disponibilizado pela ICP-Brasil, presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1o de janeiro de 1916 - Código Civil.***

ASPECTOS JURÍDICOS

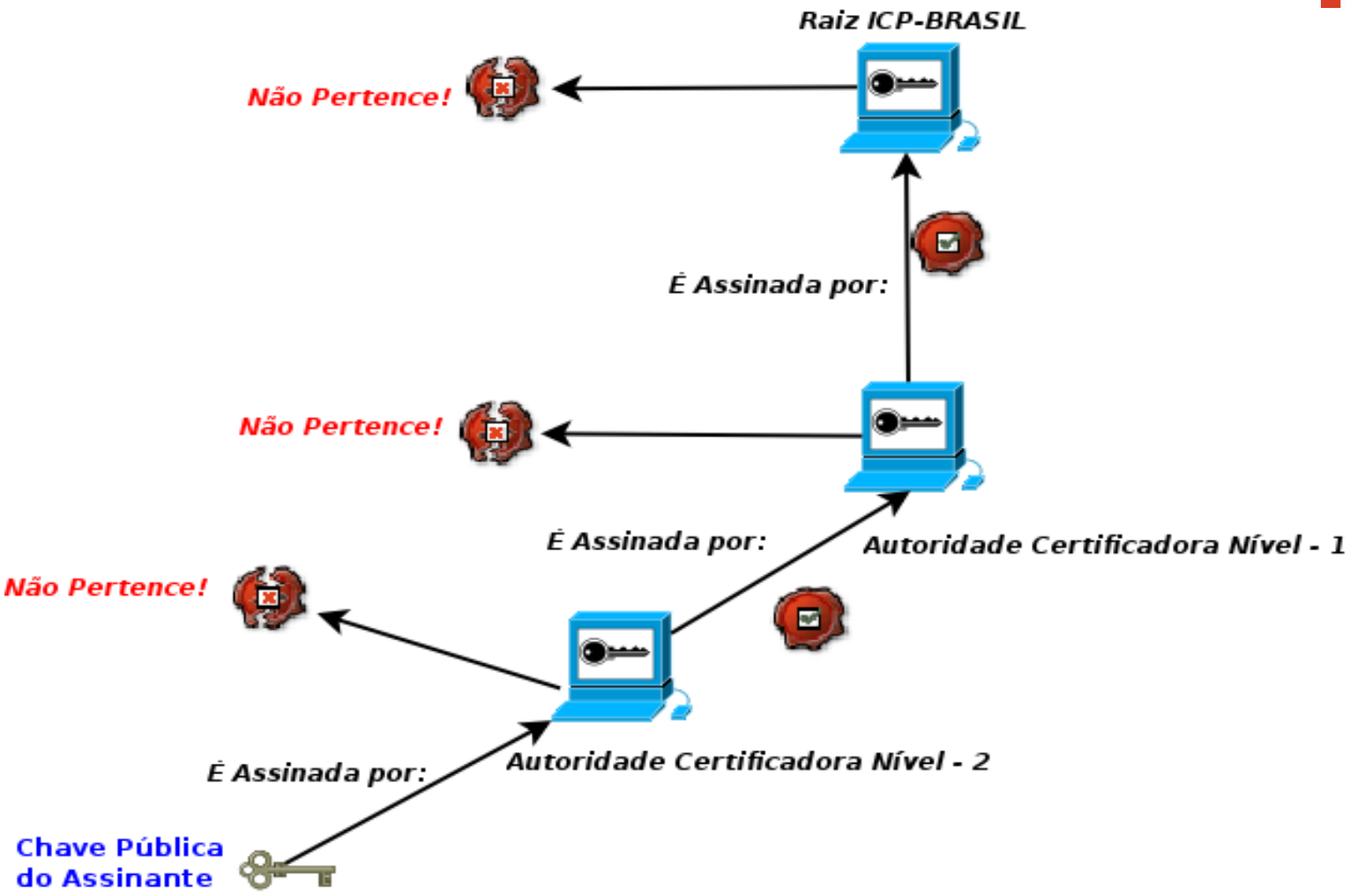
Comparativo com modelo legal estabelecido.



ASPECTOS JURÍDICOS



Exemplo de validação de Assinatura Digital



Exemplo de validação de Certificado : ICP-BRASIL

ASPECTOS JURÍDICOS

Exemplo de validação de Cadeia de certificado ICP-BRASIL.

Cadeia de Certificação:

EMERSON SACHIO SAITO
Validade do certificado: OK
Cadeia de certificacão: OK
Lista de Certificados Revogados: OK

AC CAIXA PF
Validade do certificado: OK
Cadeia de certificacão: OK
Lista de Certificados Revogados: OK

AC CAIXA
Validade do certificado: OK
Cadeia de certificacão: OK
Lista de Certificados Revogados: OK

Autoridade Certificadora Raiz Brasileira
Validade do certificado: OK
Cadeia de certificacão: OK
Lista de Certificados Revogados: OK

ASPECTOS JURÍDICOS

LEI Nº 11.419, DE 19 DE DEZEMBRO DE 2006, que dispõe sobre a informatização do processo judicial; altera a Lei no 5.869, de 11 de janeiro de 1973-Código de Processo Civil; e dá outras providências.

"*Art. 11. ...*

..§ 3o ***Os originais dos documentos digitalizados, mencionados no § 2o deste artigo, deverão ser preservados pelo seu detentor até o trânsito em julgado da sentença ou, quando admitida, até o final do prazo para interposição de ação rescisória.***

ASPECTOS JURÍDICOS

- ICP-BRASIL Já adotada pelo poder Judiciário.
  - AC-JUS
  - AC-OAB
  - Lei 11.280/2006
- Várias outras entidades públicas e privadas na estrutura.
- Ainda falta legislação, principalmente com relação a documentos convertidos para meio eletrônico.
- Já ocorreram casos de ações movidas e ganhas pela ICP-BRASIL contra soluções fora dela.
- Casos equivocados de uso de outros tipos de assinatura digital, ex: gerados exclusivamente por meios bio-métricos.

ASPECTOS JURÍDICOS

- Legislação em trâmite:
  - PLS 6.693 de 2006 (câmara) altera:
    - ***Art. 1º A Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil, passa a vigorar acrescida do art. 375-A, com a seguinte redação:***

      "Art. 375-A. O e-mail transmitido pela rede mundial de computadores - Internet, goza de presunção de veracidade quanto ao emitente e a suas declarações unilaterais de vontade, desde que certificado digitalmente nos moldes da Infra-Estrutura de Chaves Públicas Brasileira – ICP – Brasil."(NR)

      - 28/10/2008 ***Aprovada a Redação Final por Unanimidade.***
  - PLS 146 de 2007(senado): digitalização.
  - RIC (Registro de Identidade Civil)

ASPECTS JURÍDICOS

- LEA – Laboratório de Ensaios e Auditorias
  - Em 21 de outubro de 2004, o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira aprovou a Resolução nº 36 de 21/10/2004. Essa norma regulamentou o processo de homologação de sistemas e equipamentos de certificação digital no âmbito da ICPBrasil
  - Segundo a Resolução, as mídias que armazenam os certificados digitais e respectivas leitoras, além dos sistemas e equipamentos necessários à realização da certificação digital, deverão obedecer a padrões e especificações técnicas mínimas, a fim de garantir a sua interoperabilidade e a confiabilidade dos recursos de segurança da informação por eles utilizados.
  - Uma das partes mais importantes do processo de homologação é o trabalho feito pelo Laboratório de Ensaios e Auditoria - LEA. Os laboratórios são credenciados junto ao ITI para fazerem os testes e ensaios dos softwares e equipamentos.
  - http://www.iti.gov.br/twiki/bin/view/Homologacao/Concedidas

ASPECTOS CULTURAIS

- Maior responsabilidade para o usuário;
  - ✓ Assinatura de termo de responsabilidade no ato do pedido do certificado. (ICP-BRASIL)
  - ✓ Guarda do certificado e sigilo da senha
- Tecnologia e aparato tecnológico novo;
  - ✓ Tokens
  - ✓ SmartCards
  - ✓ Leitoras / Biometria
  - ✓ Falta de conhecimento -> capacitação.

ASPECTOS CULTURAIS

- Efeitos Legais.
  - Valor jurídico de documentos digitais -> não usar papel.
  - Falta de conhecimento -> orientação.
- Dificuldades e equívocos.
  - "Por enquanto" fora da ICP-BRASIL -> nunca muda
  - "Emprestar" o certificado -> somente por procuração
  - Costumes arraigados ao uso do papel.
  - Assinatura "manual" X Assinatura Digital.
  - Documento impresso = Cópia.

CONCEITOS RELACIONADOS

- <u>SEGURANÇA</u>

- Compartilha técnicas (criptografia, hash).
- Melhora com o uso de assinatura digital e certificados (https).
- Permite rastreabilidade e auditoria, com eficácia probatória (ICP-BRASIL).
- Não resolve todos os problemas!

CONCEITOS RELACIONADOS

- Workflow e BPM

  - Workflow: Controle informatizado de fluxo de trabalho (Trâmite eletrônico/ Automação de Processos).
  - BPM (Business Process Management): Gestão de Processos de Negócio, informatizado e com Workflow.

cont...

CONCEITOS RELACIONADOS

...cont

- Agrega valor legal à automação de processos burocráticos, garantindo a identidade dos agentes envolvidos no fluxo (ICP-BRASIL).
- Permite sigilo absoluto das informações/trâmites que trafegam entre os agentes.
- Elimina a necessidade do uso de papel (laudos, recibos,etc), prática comum nos finais de trâmites. (ICP-BRASIL)

CONCEITOS RELACIONADOS

- **GED/ECM**
  - GED: Gerenciamento Eletrônico de Documentos.
  - ECM (Enterprise Content Management): Gerenciamento Corporativo da Informação não estruturada.

- Aliada às técnicas já conhecidas, garante a autenticidade e integridade dos documentos eletrônicos e das informações.
- Pode também garantir o sigilo dos documentos e das informações.
- Garante a validade legal (ICP-BRASIL), já é requisito do e-ARQ-Brasil (CONARQ: Res. nº 25, de 27 de abril de 2007)

USOS

- **Autenticação de Agentes**
  - Login (senha) de rede;
  - Login em Aplicações;
  - Assinatura de logs;

- **Documentos eletrônicos**
  - Assinatura de contratos, laudos, pareceres, etc...
  - Autenticação de cópias digitais.
  - Agregar valor jurídico

USOS

- **Aplicações Habilitadas**
  - Leitores/Clientes de e-mail:
    - Assinatura digital
    - Criptografia
  - Assinadores (desktop e web);
  - Suítes de Escritório (BR-Office);

- **Sites Internet (WEB)**
  - Identificação do Site (URL, IP);
  - Protocolo seguro (https);
  - WebServices;

USOS

- **Transações Eletrônicas**

  - Formulários eletrônicos:
    - SPED (NF-e, Fiscal,Contábil);
    - procuração eletrônica;
    - ...
  - Auto atendimento;
    - Receita Federal;
    - Banco do Brasil;
    - ...

USOS

- **<u>Informações fidedignas (legalmente confiáveis).</u>**

  - Despachos eletrônicos:
    - Alguns sites da Justiça,
    - ...
  - Alguns diários oficiais dos Estados
    - DIOE-PR (www.documentos.dioe.pr.gov.br),
    - ...

SOLUÇÕES.

- Solução da CELEPAR: **Tabelião-Pinhão**.
  - Autenticação/Login
  - Assinaturas digitais nos formatos:
    - PKCS#7 (CMS).
    - XML Enveloped (NF-e).
    - XML Enveloping (web-services).
  - Manipulação e Validações de Certificados
  - Manipulação e Validações de LCR (Lista de certificados Revogados)

SOLUÇÕES.

- Solução da CELEPAR: **Tabelião-Pinhão**.
  - NF-e (Recepção pela SEFA-PR)
  - DIOE – Premio CONIP 2008, A-Rede.
  - Execução Fiscal (SEFA-PGE)
  - PRODAM (AM)

APLICATIVOS/FERRAMENTAS

- Lista de aplicativos no site PINHÃO-PARANÁ
  http://www.frameworkpinhao.pr.gov.br/
- Estão disponíveis também vídeos de captura de telas (*screencast*) de todas as ferramentas e manuais.

TEMPESTIVIDADE DIGITAL

- Carimbo de Tempo

Documento eletrônico emitido por uma parte confiável, que serve como evidência de que uma informação digital existia numa determinada data e hora no passado. Deverá obrigatoriamente estar ligado logicamente ao conteúdo eletrônico que atesta, nos mesmos formatos de uma assinatura digital.

TEMPESTIVIDADE DIGITAL

A autenticidade do carimbo deve ser garantida por uma assinatura digital de uma autoridade confiável.

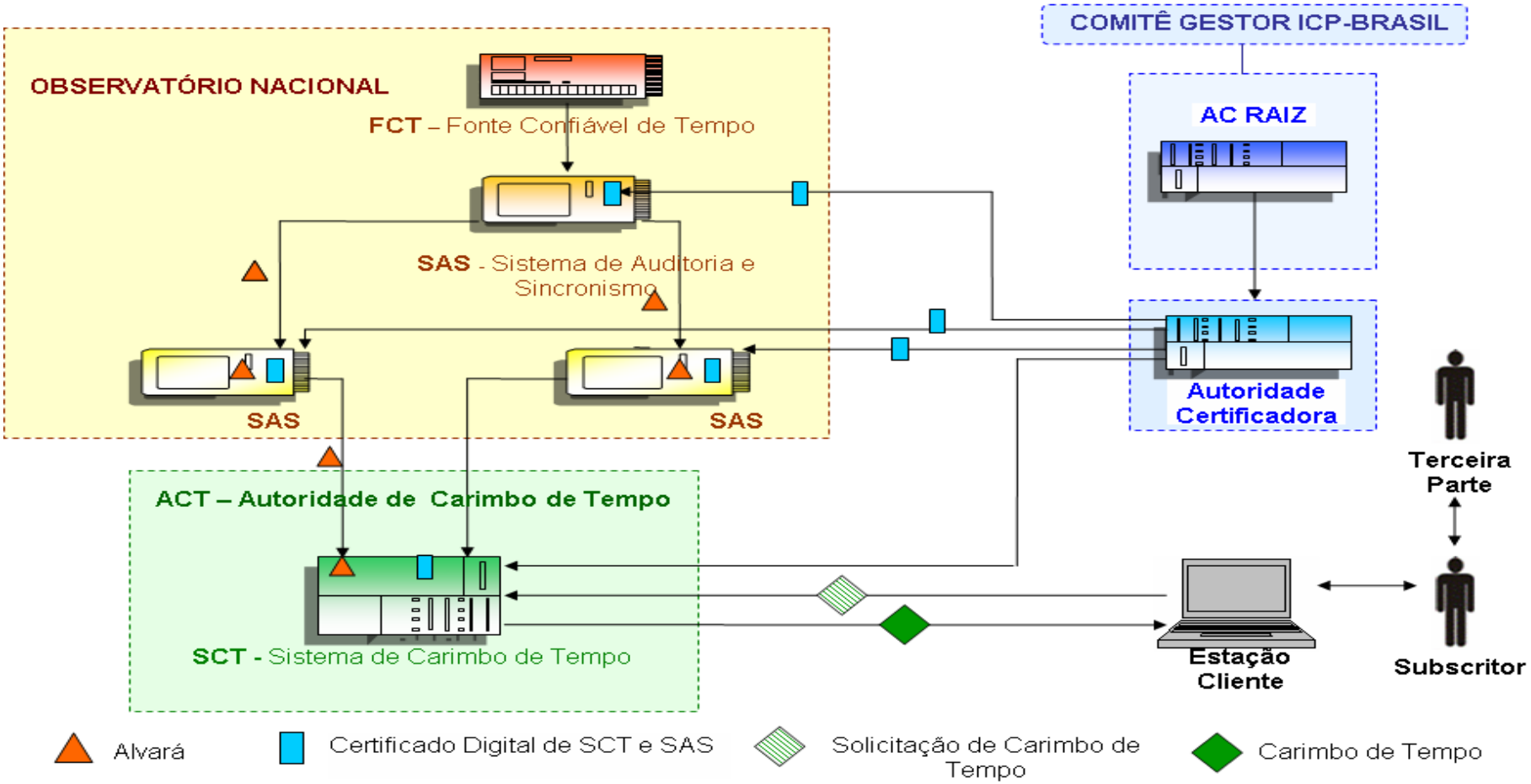
Deve possuir uma fonte de tempo confiável e legítima, no caso do Brasil é o Observatório Nacional.

Deverá estar normatizado pela ICP-BRASIL.

Prevê a figura da Autoridade de Carimbo de Tempo (ACT).

TEMPESTIVIDADE DIGITAL

Carimbo de Tempo na ICP-Brasil



Fonte: ITI

Pinhão
PARANÁ

GOVERNO DO
PARANÁ

SEAE
SECRETARIA DE ESTADO DE ASSUNTOS ESTRATÉGICOS

CELEPAR
INFORMÁTICA
do PARANÁ

CELEPAR
INFORMÁTICA
do PARANÁ