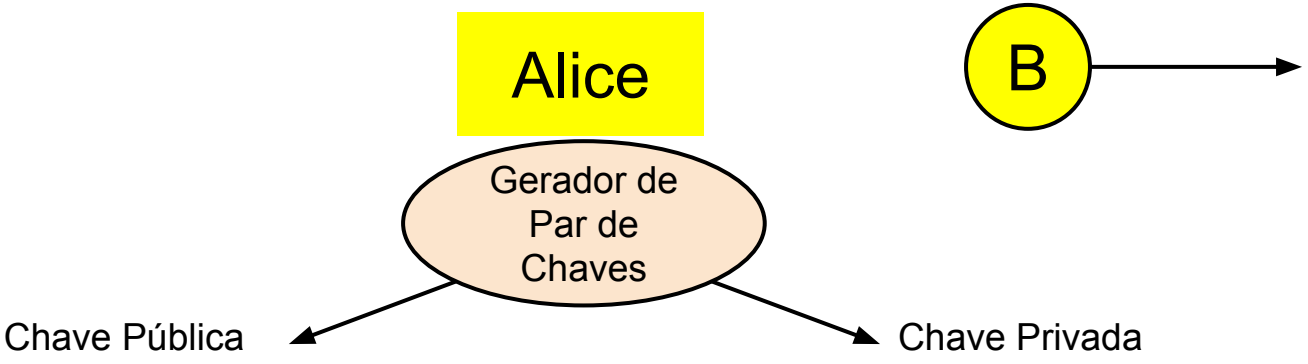
Assinatura Digital

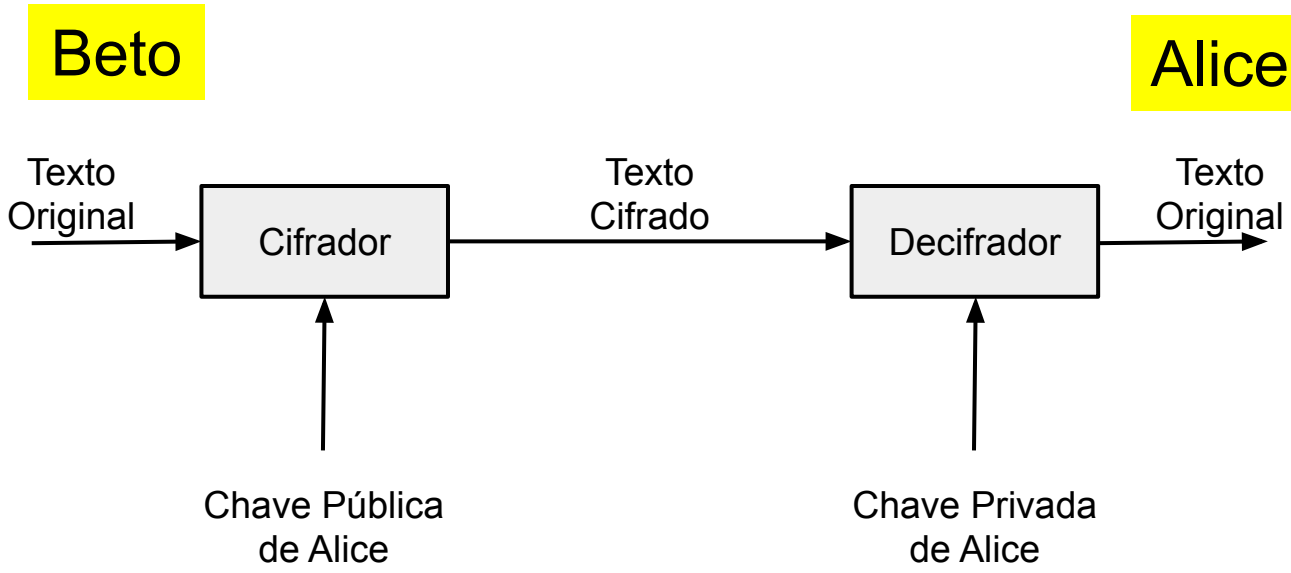
Prof. Ricardo Custódio, Dr.
ricardo.custodio@ufsc.br

Abril de 2019

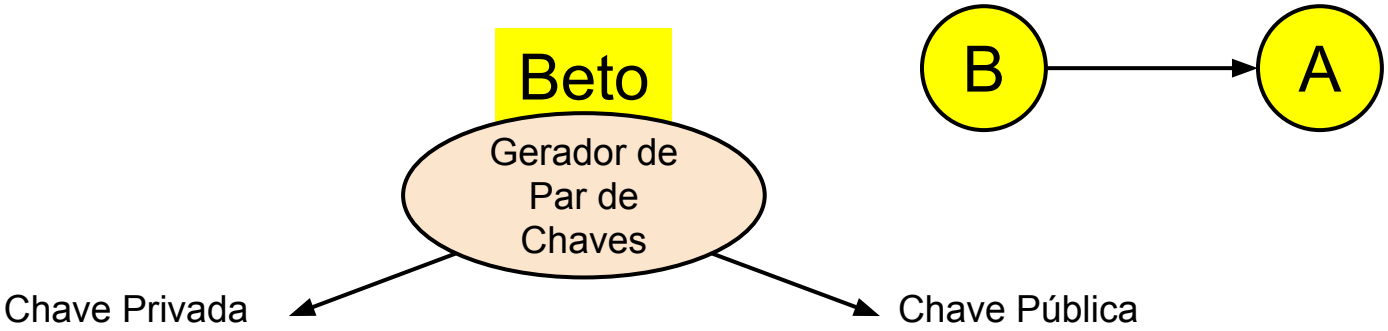
Criptografia Assimétrica

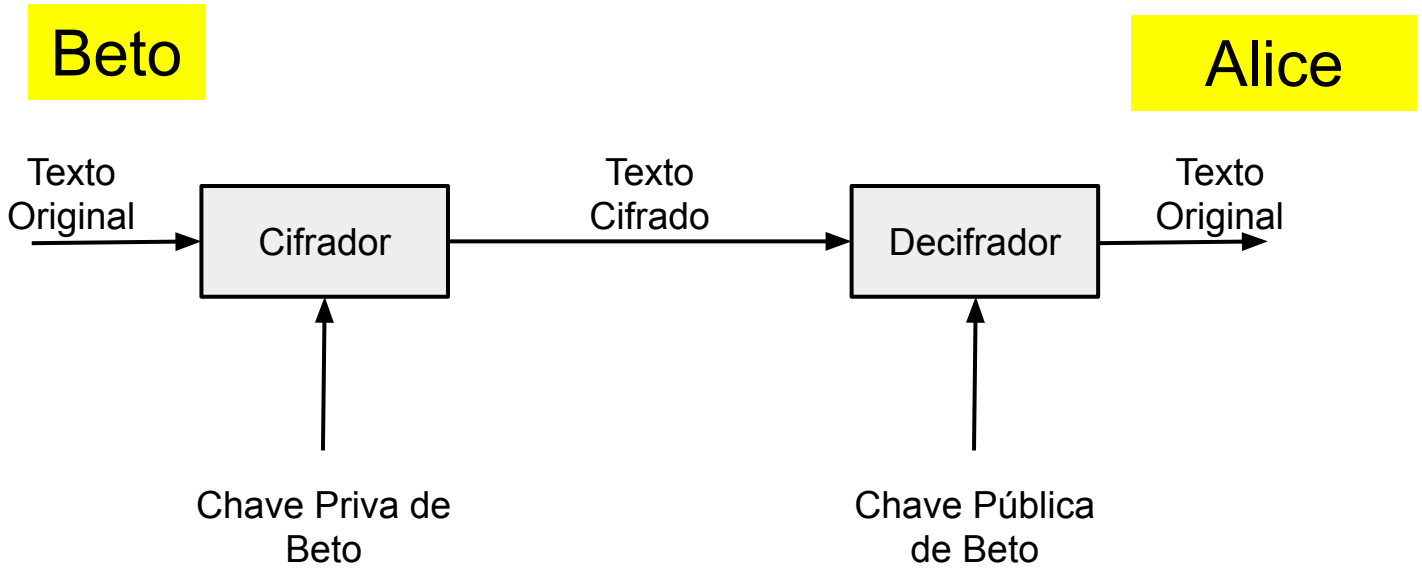
Sigilo



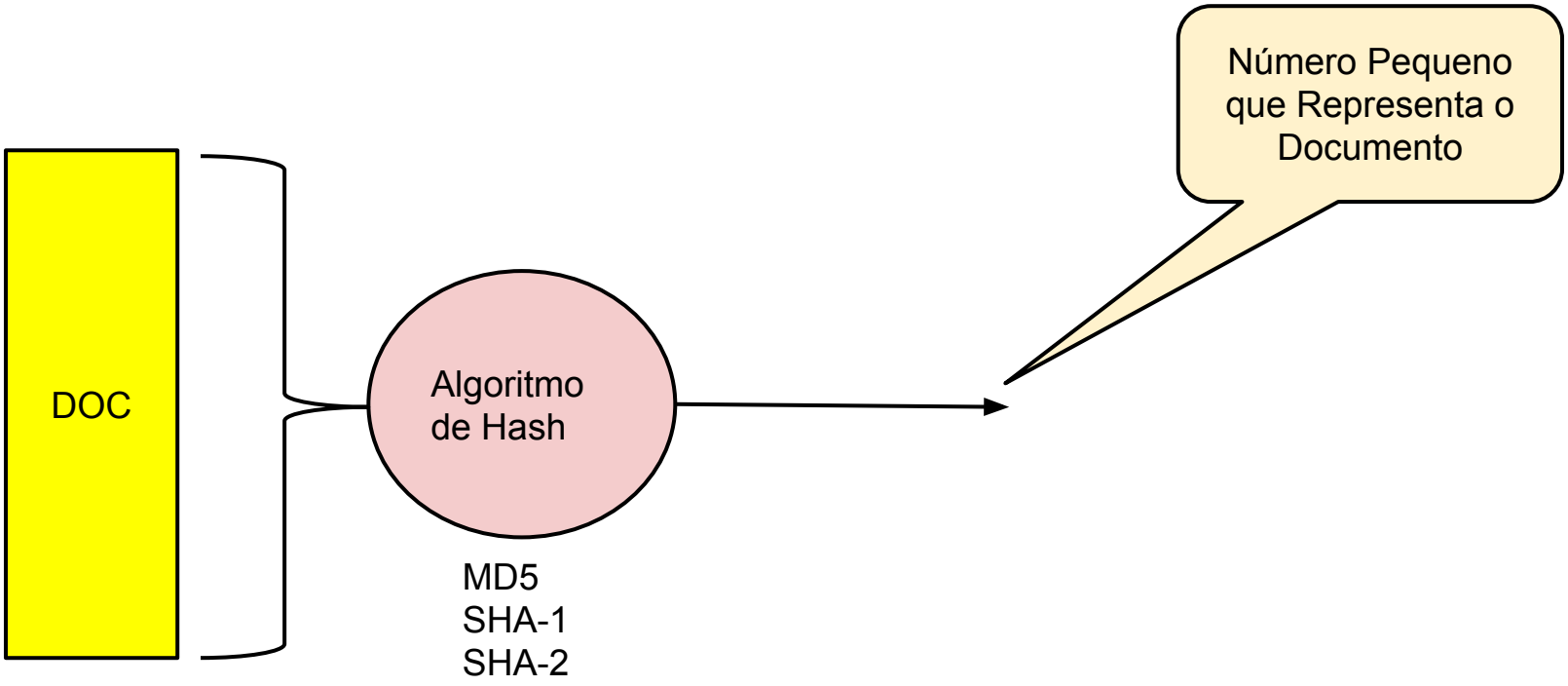


Criptografia Assimétrica
Autenticação





Algoritmos de Hash



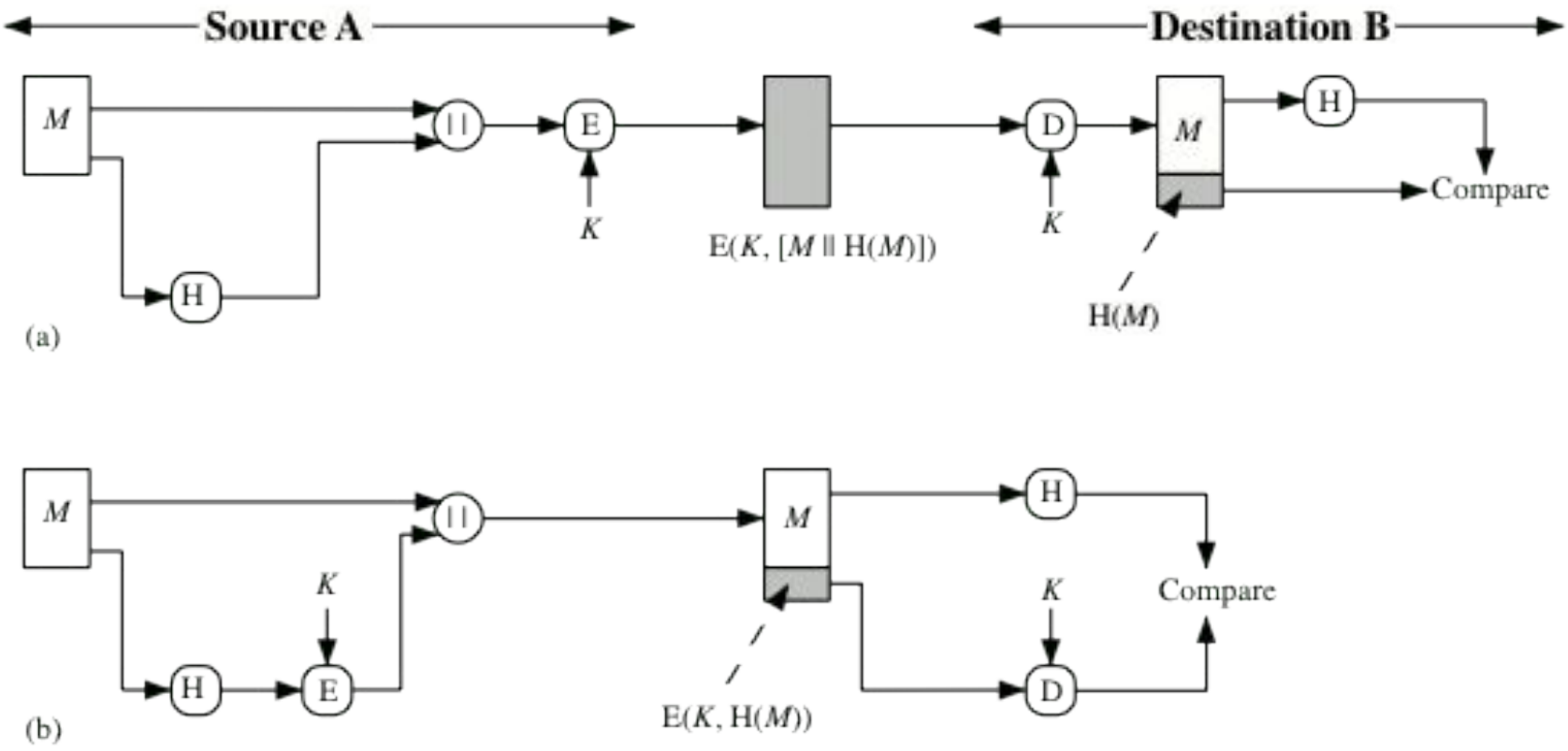
Exemplo SHA-1

3F:F4:E3:C6:7B:2D:29:FC:A4:85:93:E2:BA:96:17:55:3C:41:AC:F2

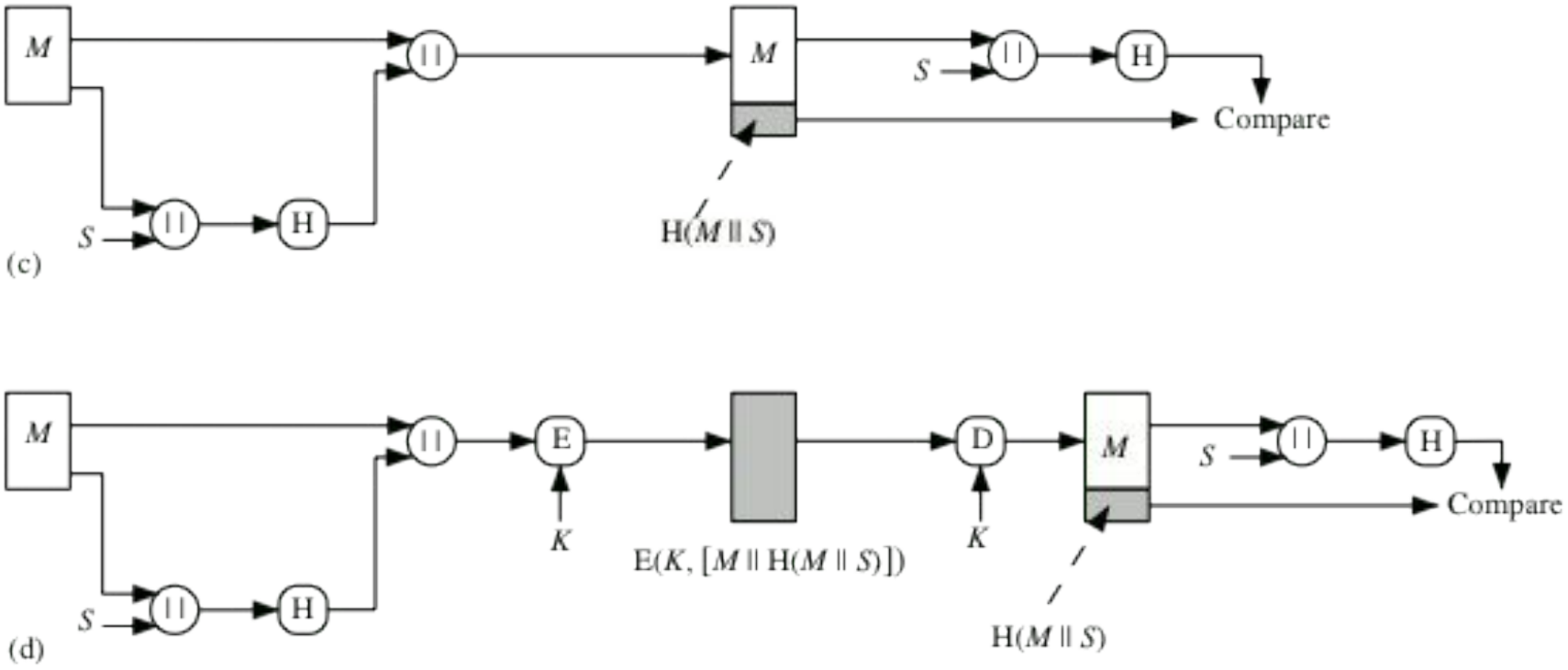
Requisitos para Funções Hash H

Requisito	Descrição
Tamanho da Entrada Variável	H pode ser aplicada a um bloco de dados de qualquer tamanho
Tamanho da Saída Fixo	H produz uma saída de tamanho fixo
Eficiência	H(x) é relativamente simples de computar
Resistência a pré-imagem	Dado h, é computacionalmente inviável encontrar y tal que H(y) = x
Resistência à segunda pré-imagem (resitência a colisão fraca)	Para um dado x, é computacionalmente inviável encontrar y ≠ x com H(x) = H(y)
Resistência à Colisão (resistência a colisão forte)	É computacionalmente inviável encontrar pares (x,y) tal qye H(x)=H(y)
Saída pseudo-randômica	Saída H passa nos testes padronizados de psenudorandomicidade

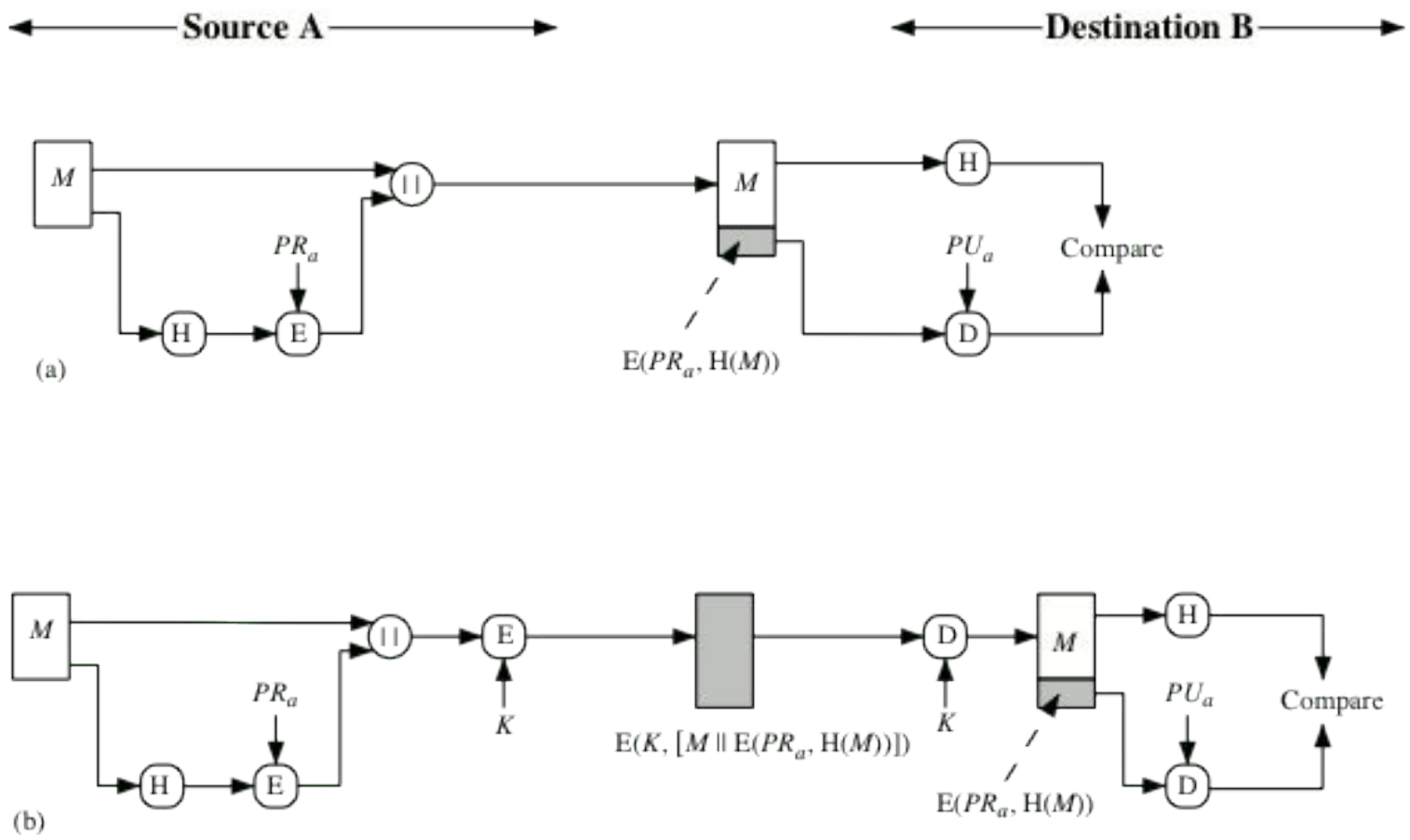
Função Hash para Autenticação de Mensagens



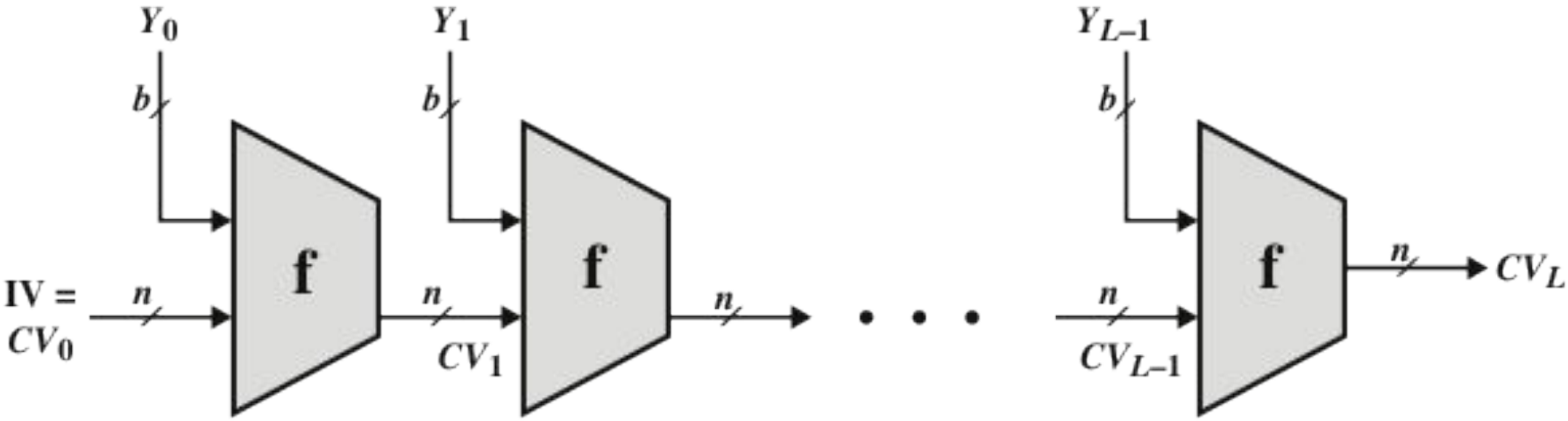
Função Hash com Senha para Autenticação de Mensagens



Função Hash com Senha para Autenticação de Mensagens



Construção de Merkle-Damgard



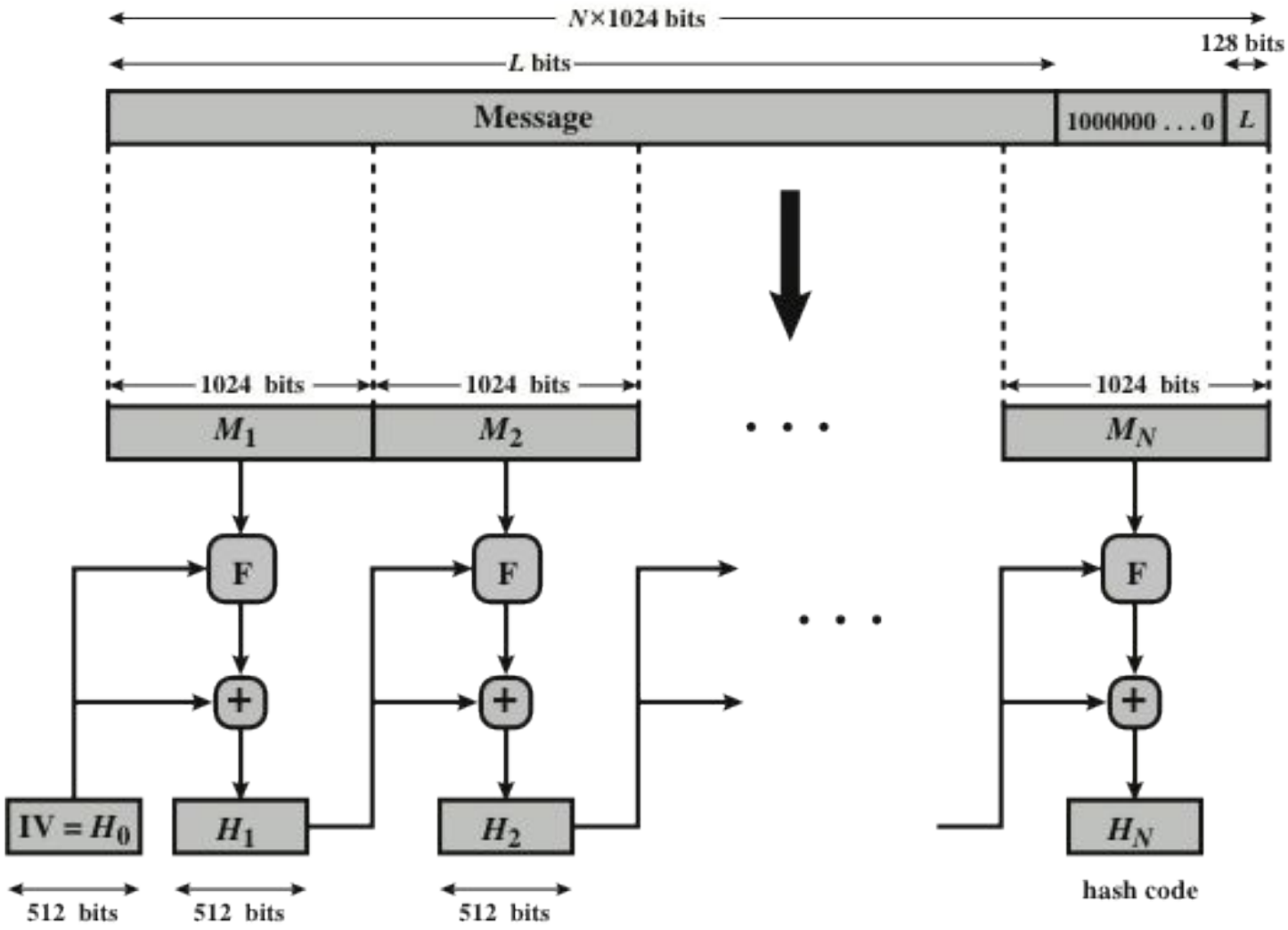
IV = Initial value
CV_i = chaining variable
Y_i = ith input block
f = compression algorithm

L = number of input blocks
n = length of hash code
b = length of input block

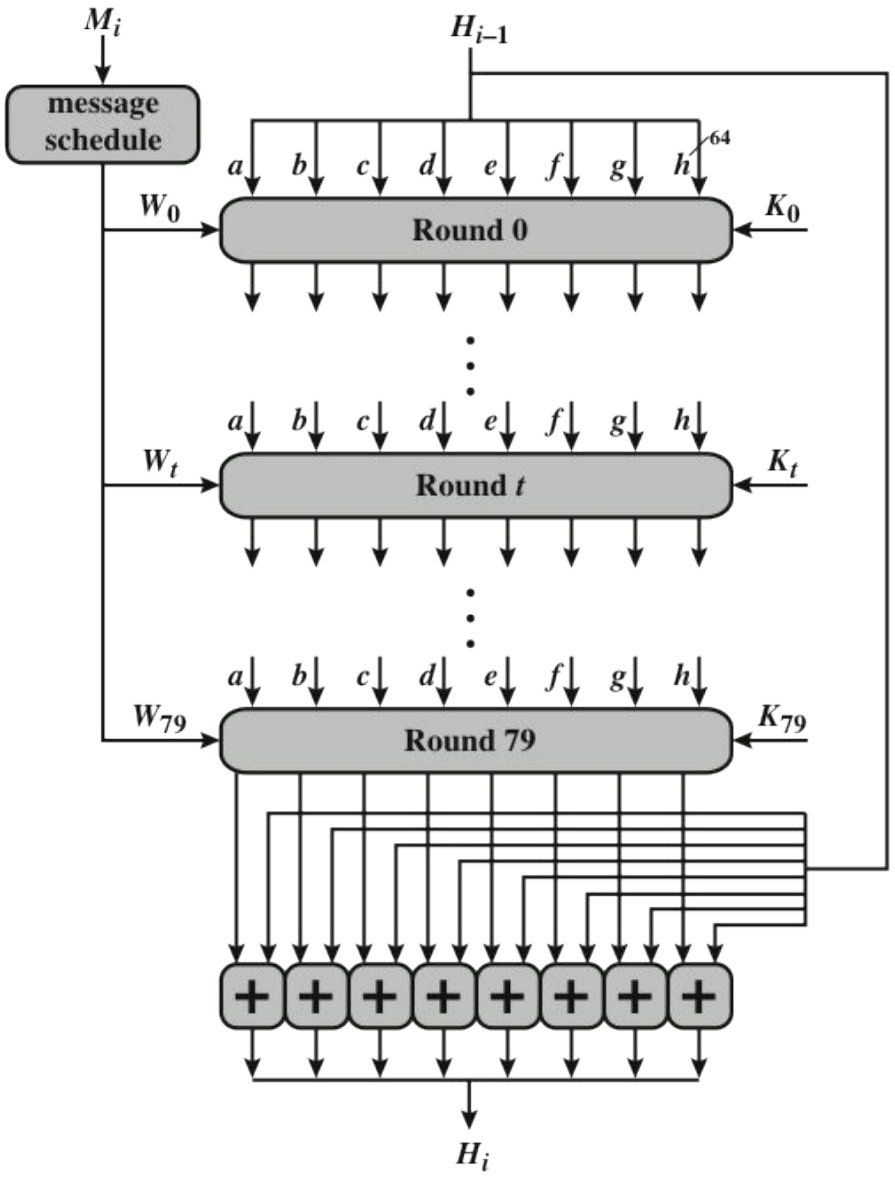
Parâmetro do Secure Hash Algorithm (SHA)

	SHA-1	SHA-224	SHA-256	SHA-384	SHA-512
Tamanho da Saída	160	224	256	384	512
Tamanho da Entrada	$<2^{64}$	$<2^{64}$	$<2^{64}$	$<2^{128}$	$<2^{128}$
Tamanho do Bloco	512	512	512	1024	1024
Tamanho da Palavra	32	32	32	64	64
Número de Passos	80	64	64	80	80

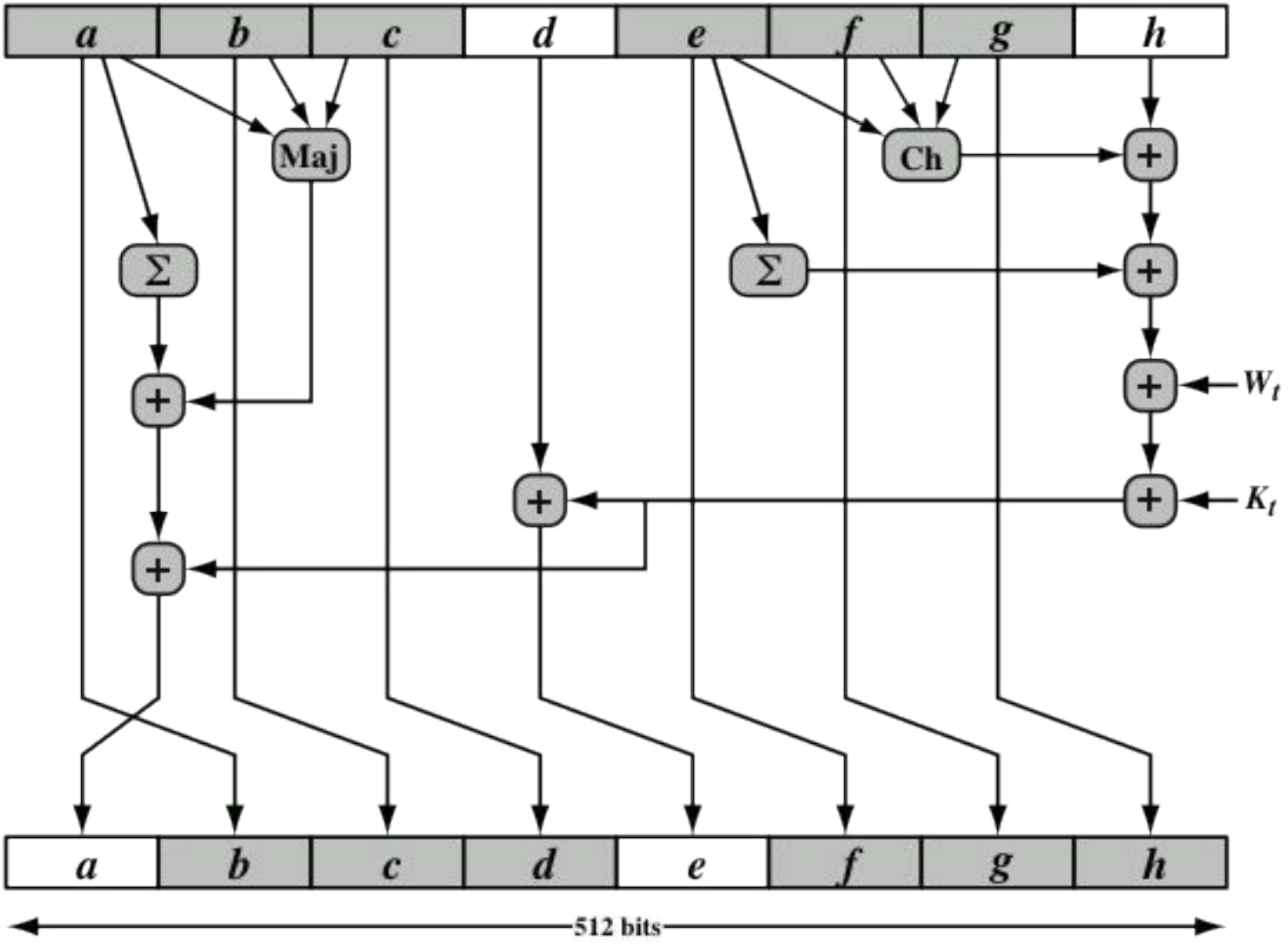
Hash SHA-512


N×1024 bits
128 bits
L bits
Message
1000000 . . . 0
L
1024 bits
1024 bits
1024 bits
M1
M2
MN
F
F
F
IV = H0
H1
H2
HN
512 bits
512 bits
512 bits
hash code

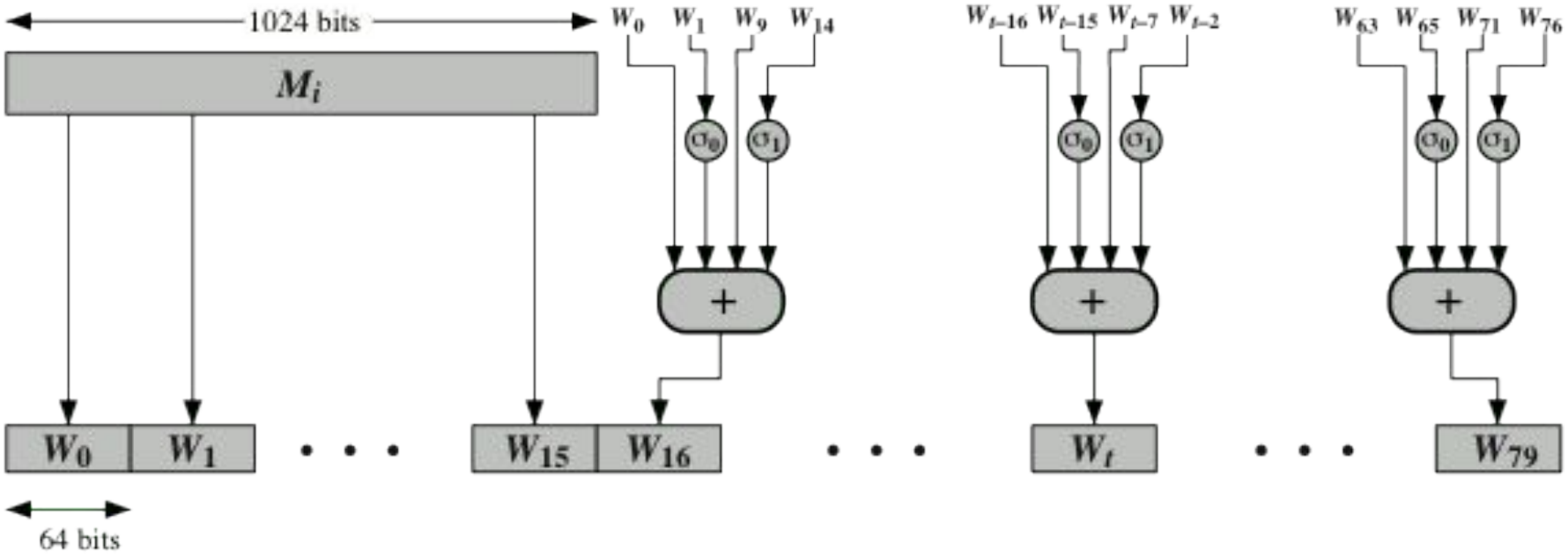
Função de Compressão SHA-512

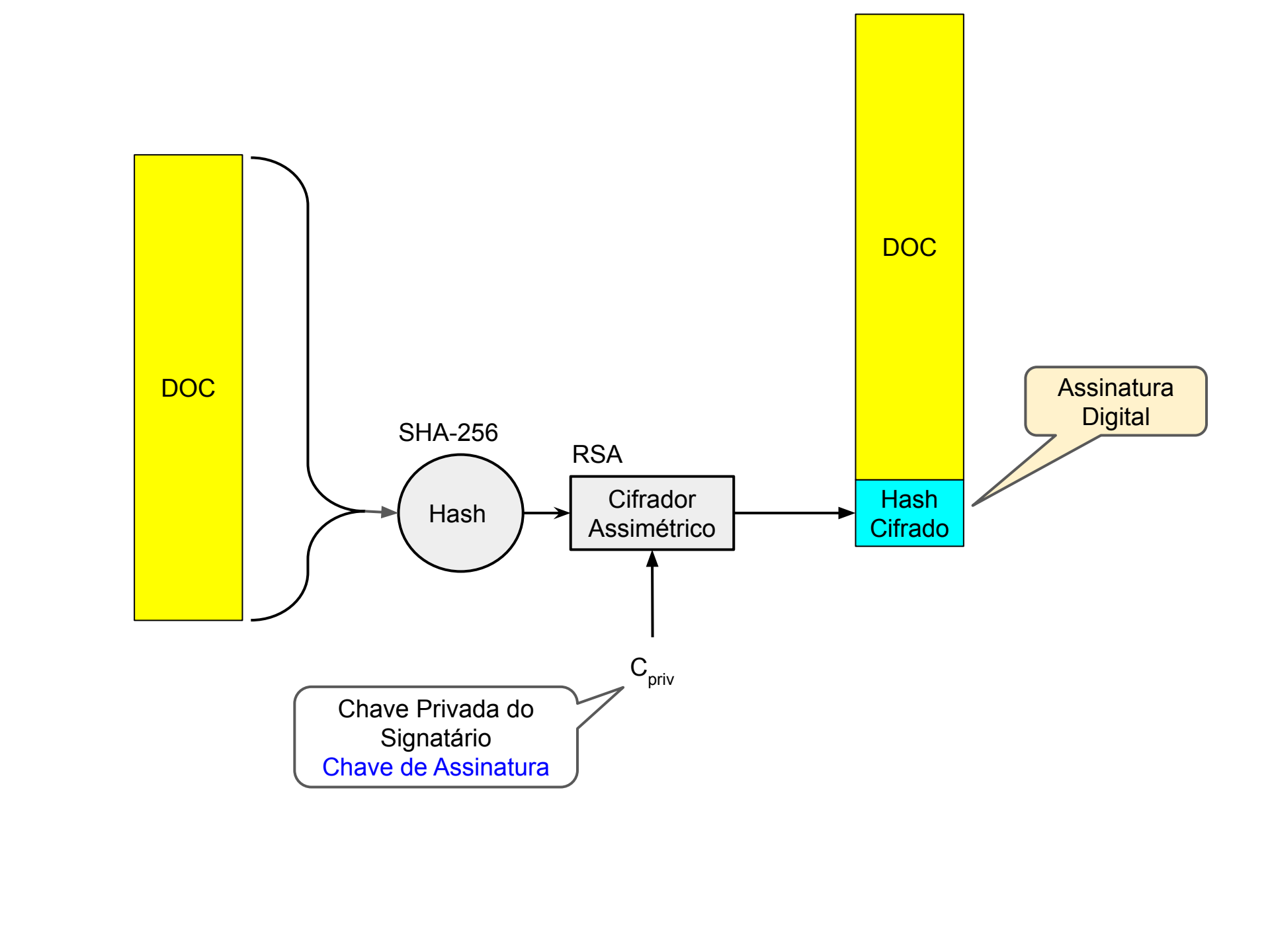


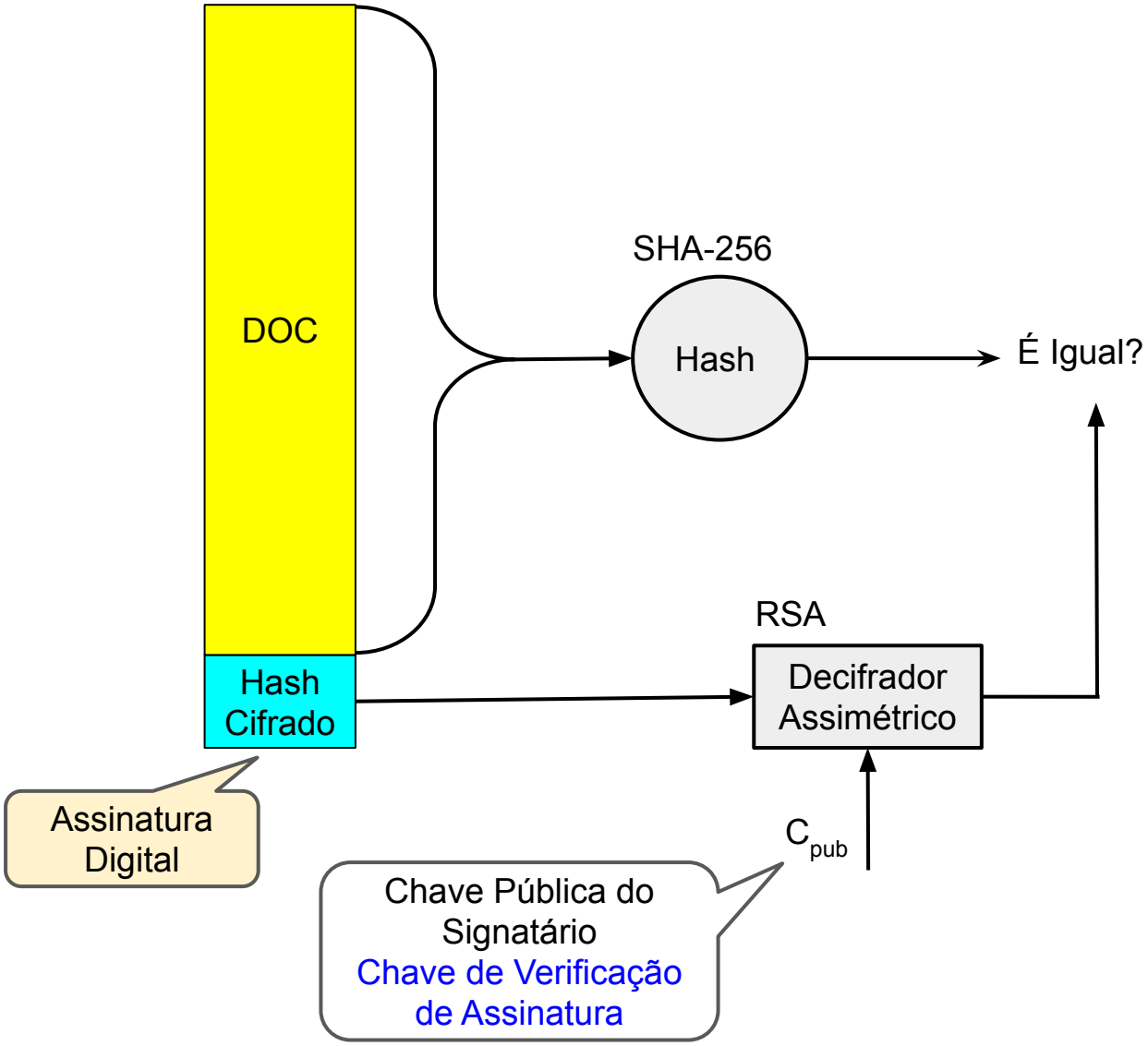
Um Passo do SHA-512



Sequência de Entradas




DOC
DOC
SHA-256
Hash
RSA
Cifrador
Assimétrico
DOC
Hash
Cifrado
Assinatura
Digital
C priv
Chave Privada do
Signatário
Chave de Assinatura


DOC
SHA-256
Hash
É Igual?
RSA
Hash Cifrado
Decifrador Assimétrico
Assinatura Digital
C_{pub}
Chave Pública do Signatário
Chave de Verificação de Assinatura

Assinaturas de Próprio Punho

Presidência da República
Secretaria de Relações Institucionais
Esplanada dos Ministérios – Bloco H – Anexo II - Sala 24 - Térreo- 70150-090 – Brasília – DF
Tel.: (61) 411-1127/1042 – sripr@planalto.gov.br

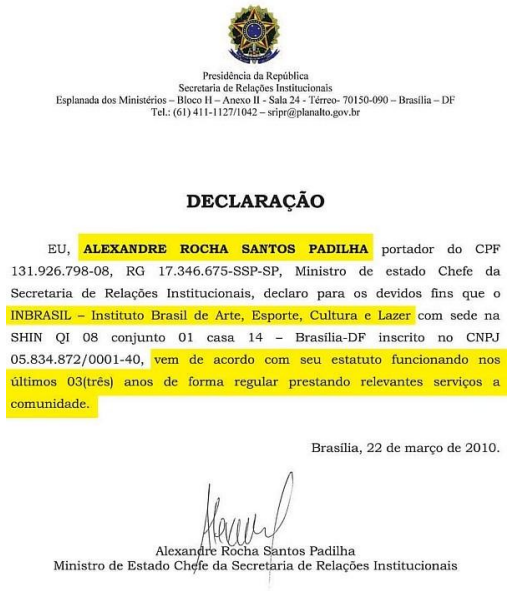
DECLARAÇÃO

EU, **ALEXANDRE ROCHA SANTOS PADILHA** portador do CPF 131.926.798-08, RG 17.346.675-SSP-SP, Ministro de estado Chefe da Secretaria de Relações Institucionais, declaro para os devidos fins que o INBRASIL – Instituto Brasil de Arte, Esporte, Cultura e Lazer com sede na SHIN QI 08 conjunto 01 casa 14 – Brasília-DF inscrito no CNPJ 05.834.872/0001-40, vem de acordo com seu estatuto funcionando nos últimos 03(três) anos de forma regular prestando relevantes serviços a comunidade.

Brasília, 22 de março de 2010.

Alexandre Rocha Santos Padilha
Ministro de Estado Chefe da Secretaria de Relações Institucionais

Assinatura Digital



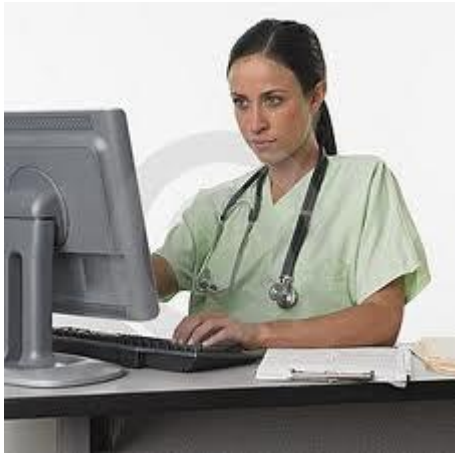
Presidência da República
Secretaria de Relações Institucionais
Esplanada dos Ministérios – Bloco H – Anexo II – Sala 24 - Térreo- 70150-090 – Brasília – DF
Tel.: (61) 411-1127/1042 – sripr@planalto.gov.br

DECLARAÇÃO

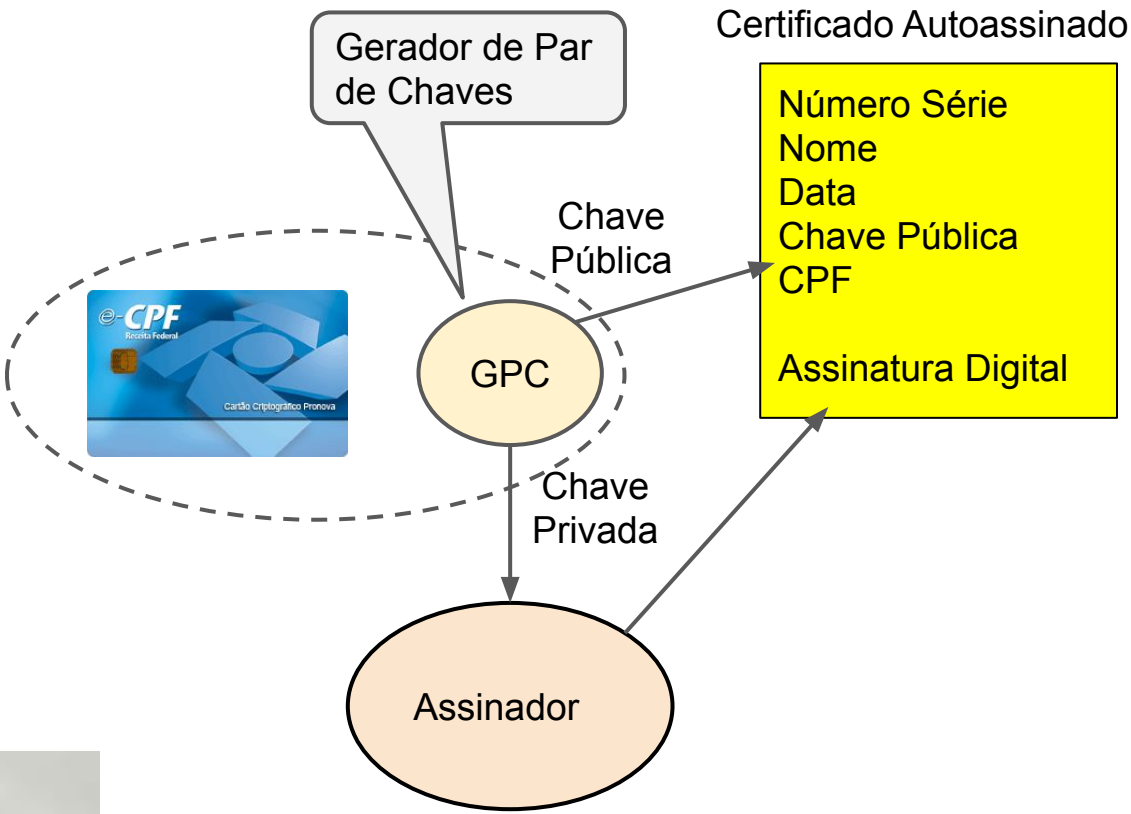
EU, **ALEXANDRE ROCHA SANTOS PADILHA** portador do CPF 131.926.798-08, RG 17.346.675-SSP-SP, Ministro de estado Chefe da Secretaria de Relações Institucionais, declaro para os devidos fins que o INBRASIL – Instituto Brasil de Arte, Esporte, Cultura e Lazer com sede na SHIN QI 08 conjunto 01 casa 14 – Brasília-DF inscrito no CNPJ 05.834.872/0001-40, vem de acordo com seu estatuto funcionando nos últimos 03(três) anos de forma regular prestando relevantes serviços a comunidade.

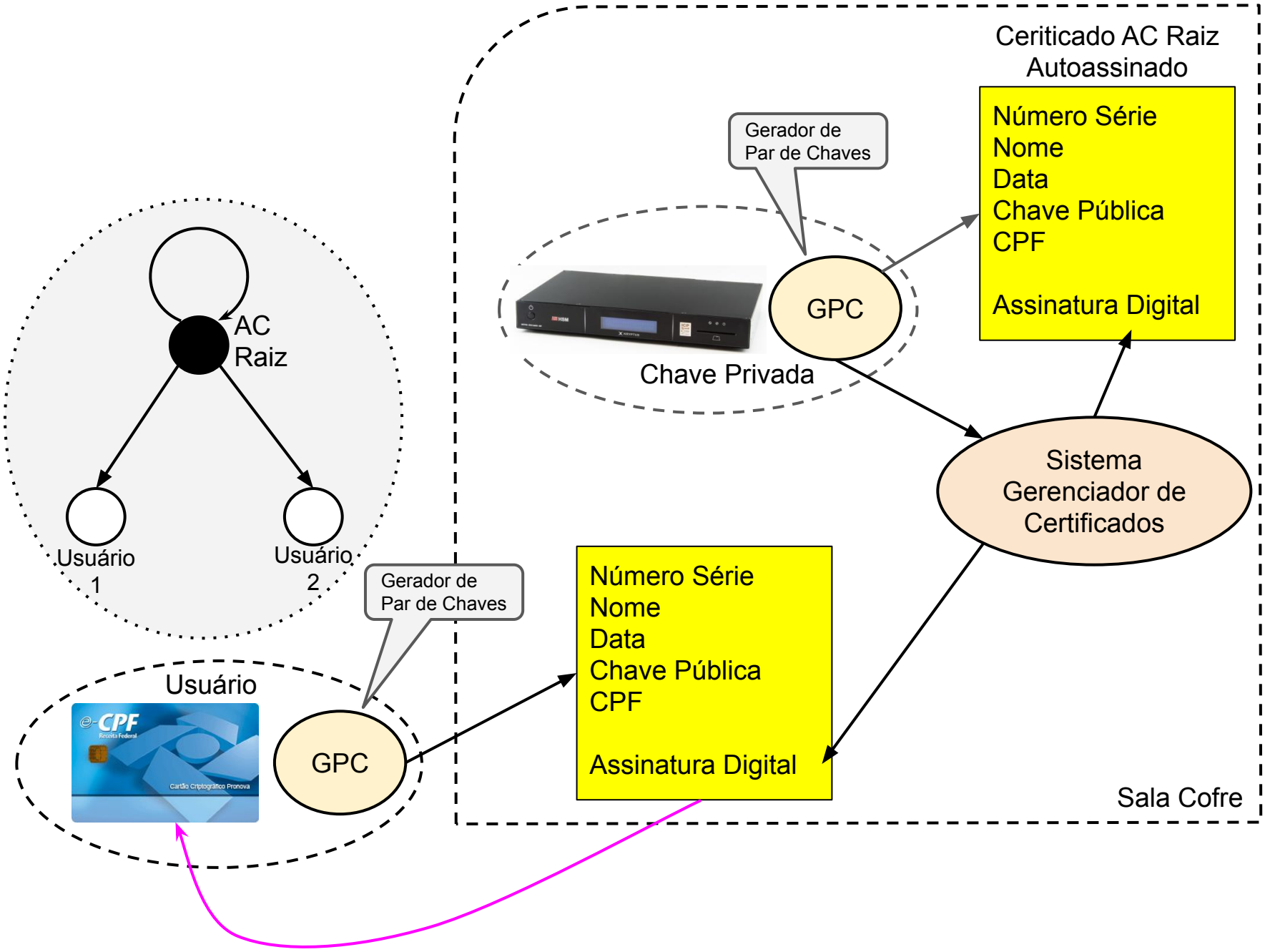
Brasília, 22 de março de 2010.

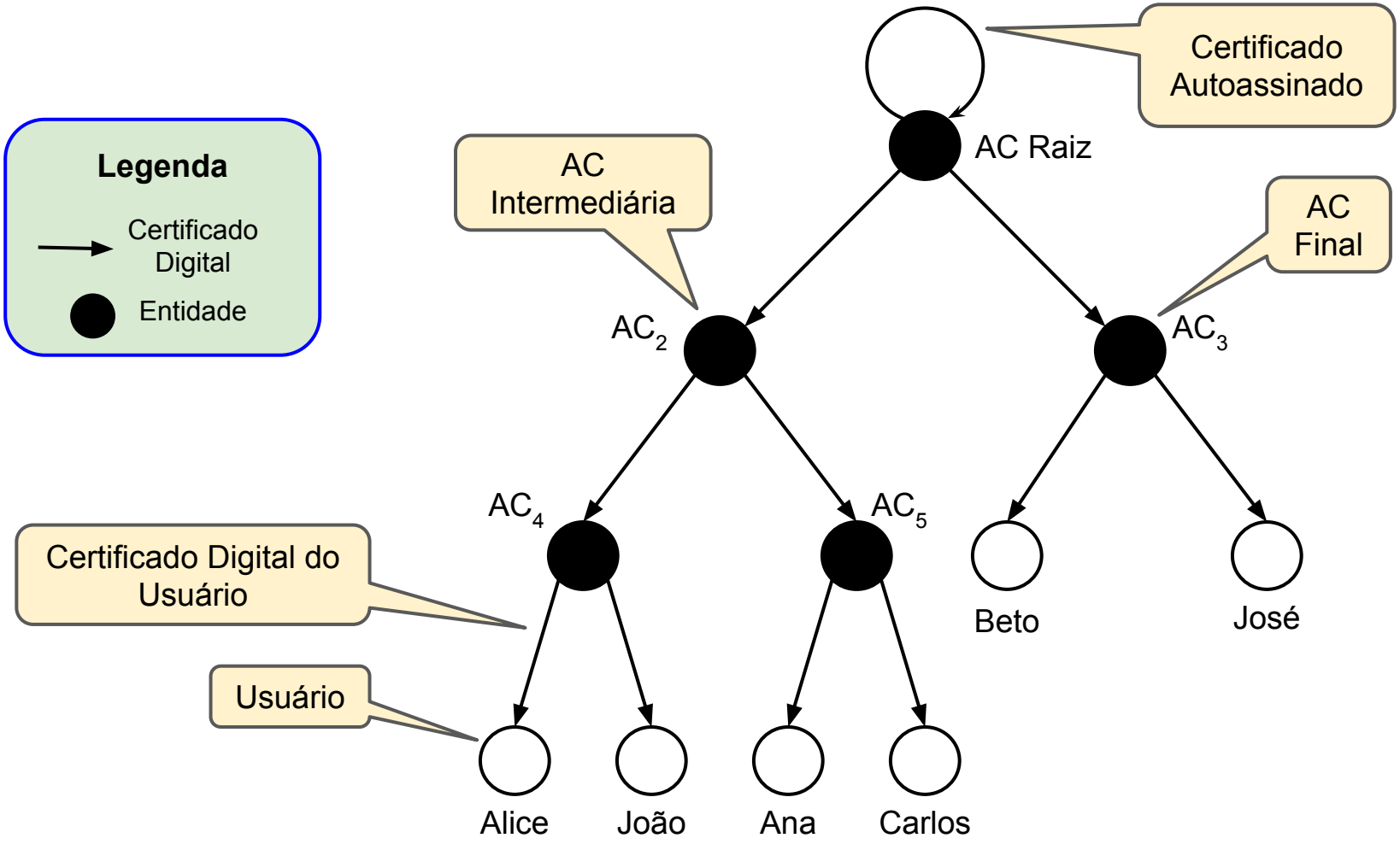
Alexandre Rocha Santos Padilha
Ministro de Estado Chefe da Secretaria de Relações Institucionais

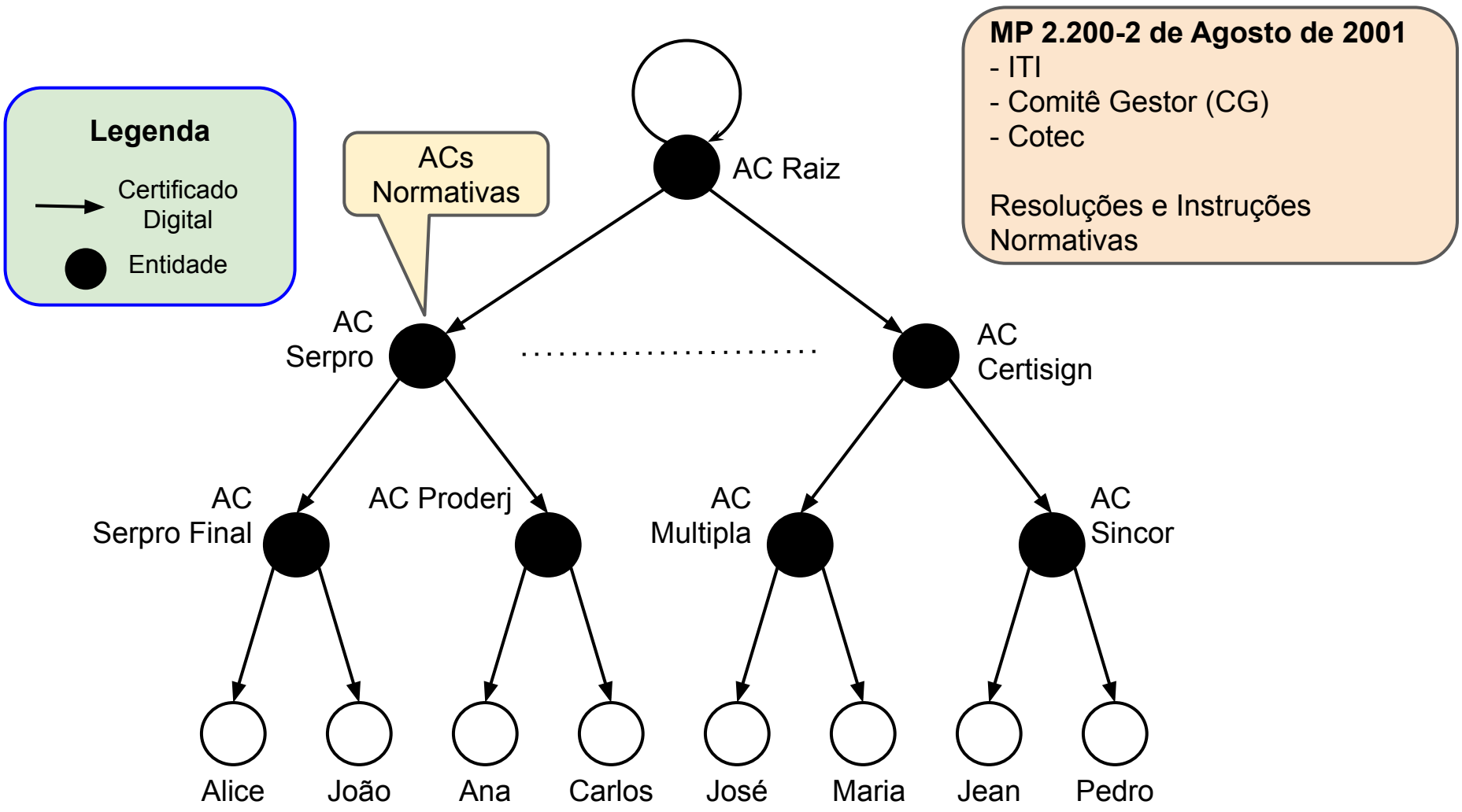


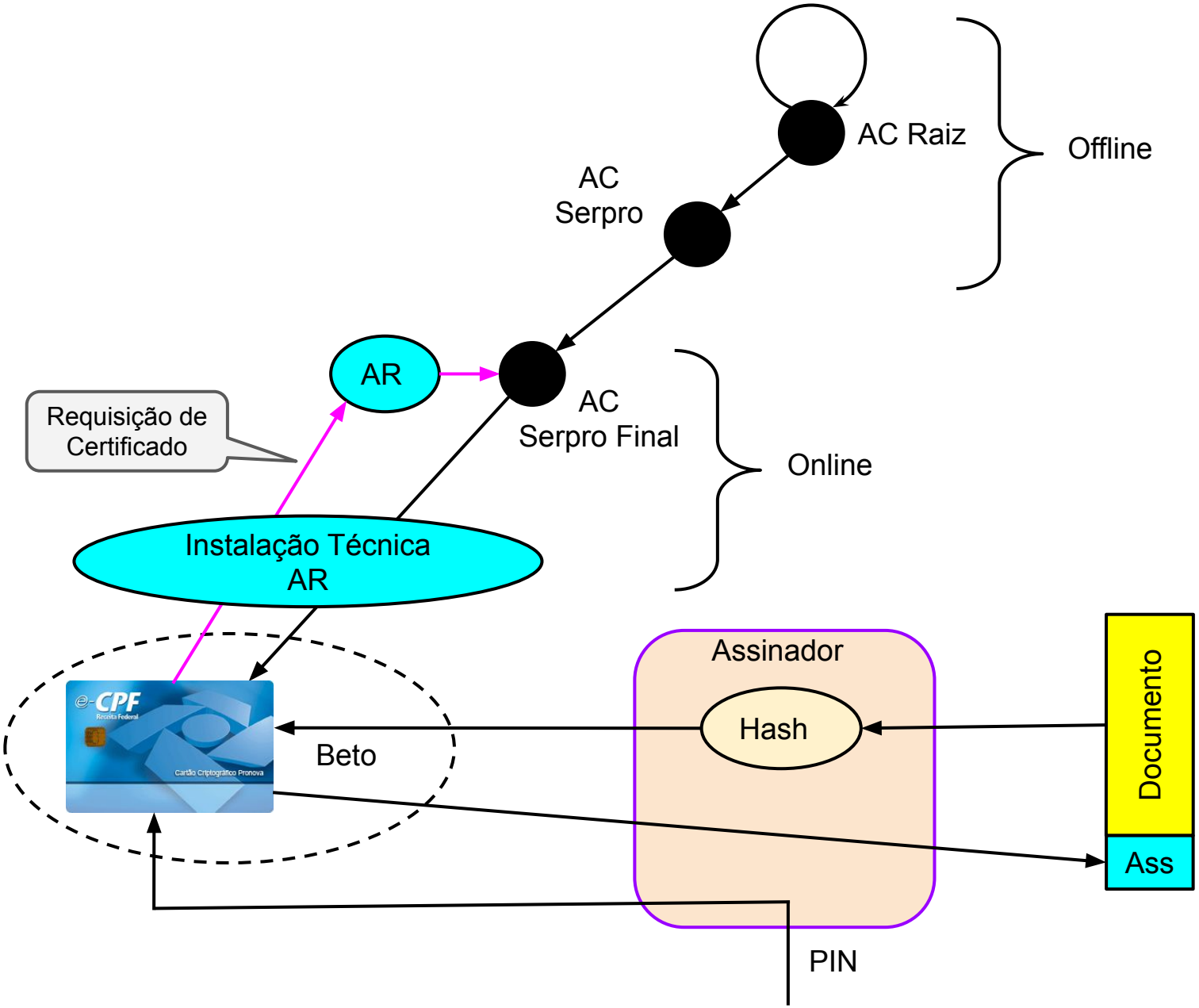
Certificado Digital
Autoassinado

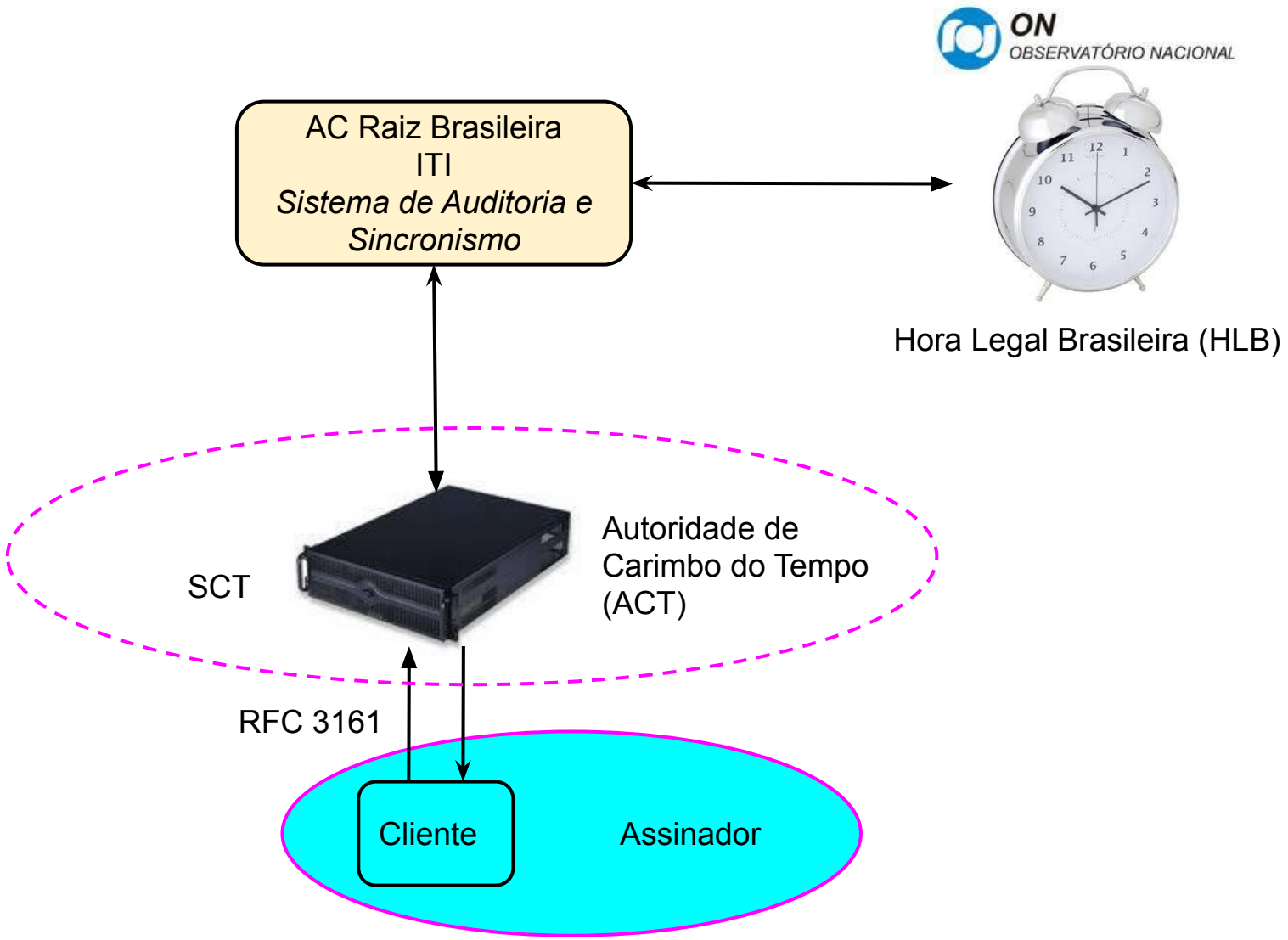


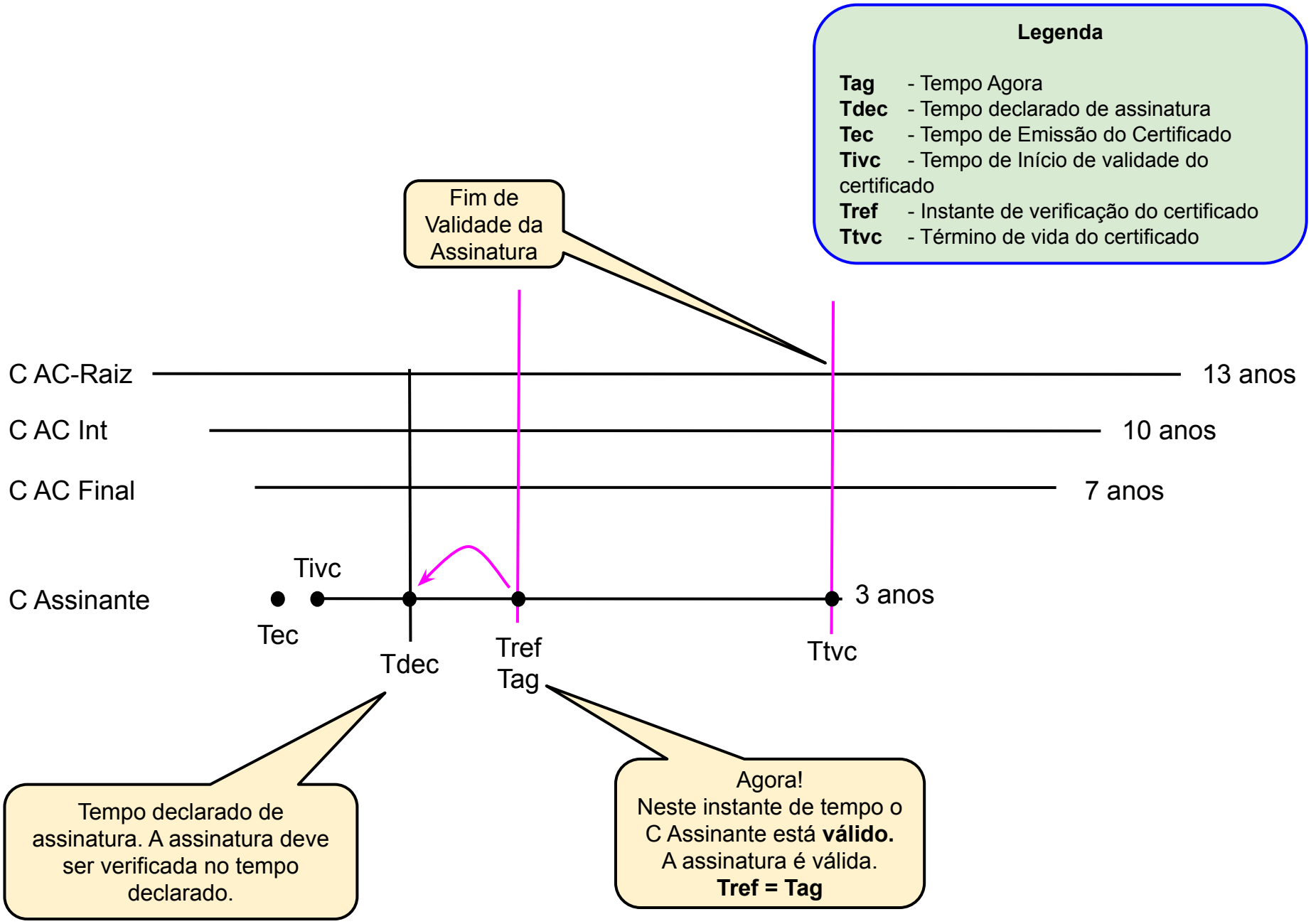

Ceriticado AC Raiz
Autoassinado
Número Série
Nome
Data
Chave Pública
CPF
Assinatura Digital
Gerador de
Par de Chaves
GPC
Chave Privada
AC
Raiz
Usuário
1
Usuário
2
Sistema
Gerenciador de
Certificados
Gerador de
Par de Chaves
Usuário
GPC
Número Série
Nome
Data
Chave Pública
CPF
Assinatura Digital
Sala Cofre

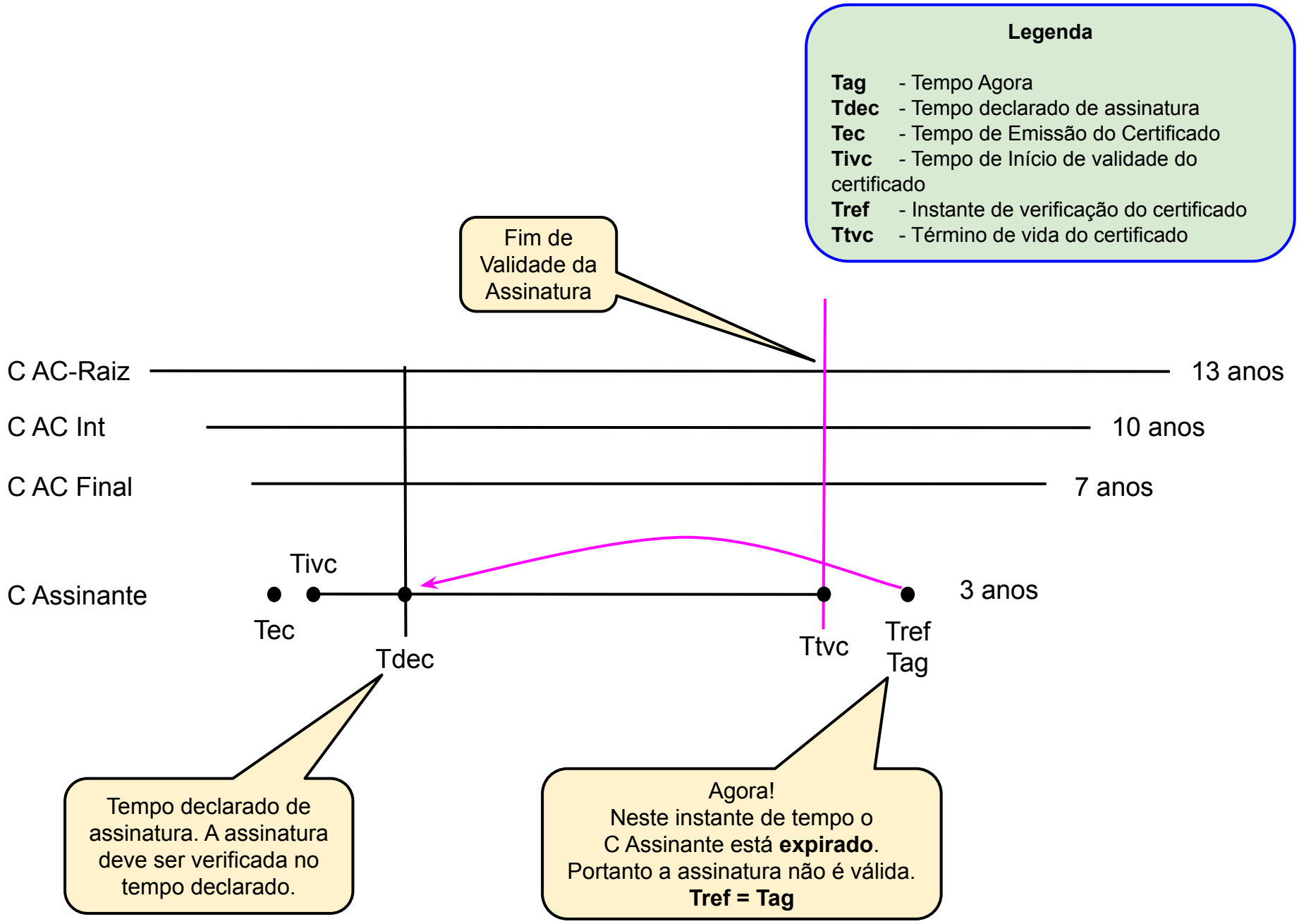

Legenda
Certificado Digital
Entidade
Certificado Autoassinado
AC Raiz
AC Intermediária
AC Final
AC2
AC3
AC4
AC5
Certificado Digital do Usuário
Usuário
Beto
José
Alice
João
Ana
Carlos

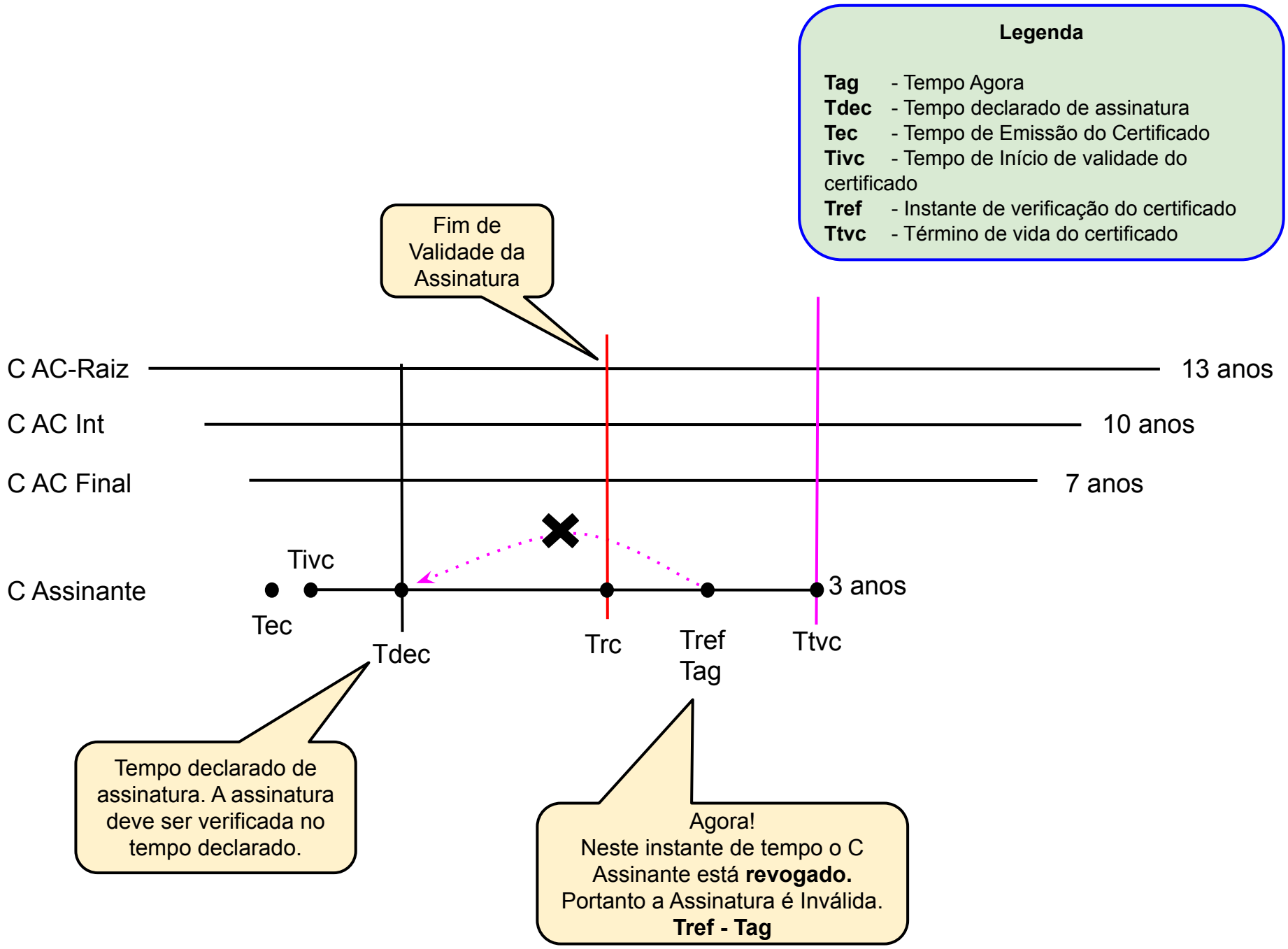

Legenda
Certificado Digital
Entidade
ACs Normativas
AC Raiz
MP 2.200-2 de Agosto de 2001
- ITI
- Comitê Gestor (CG)
- Cotec
Resoluções e Instruções Normativas
AC Serpro
AC Certisign
AC Serpro Final
AC Proderj
AC Multipla
AC Sincor
Alice
João
Ana
Carlos
José
Maria
Jean
Pedro

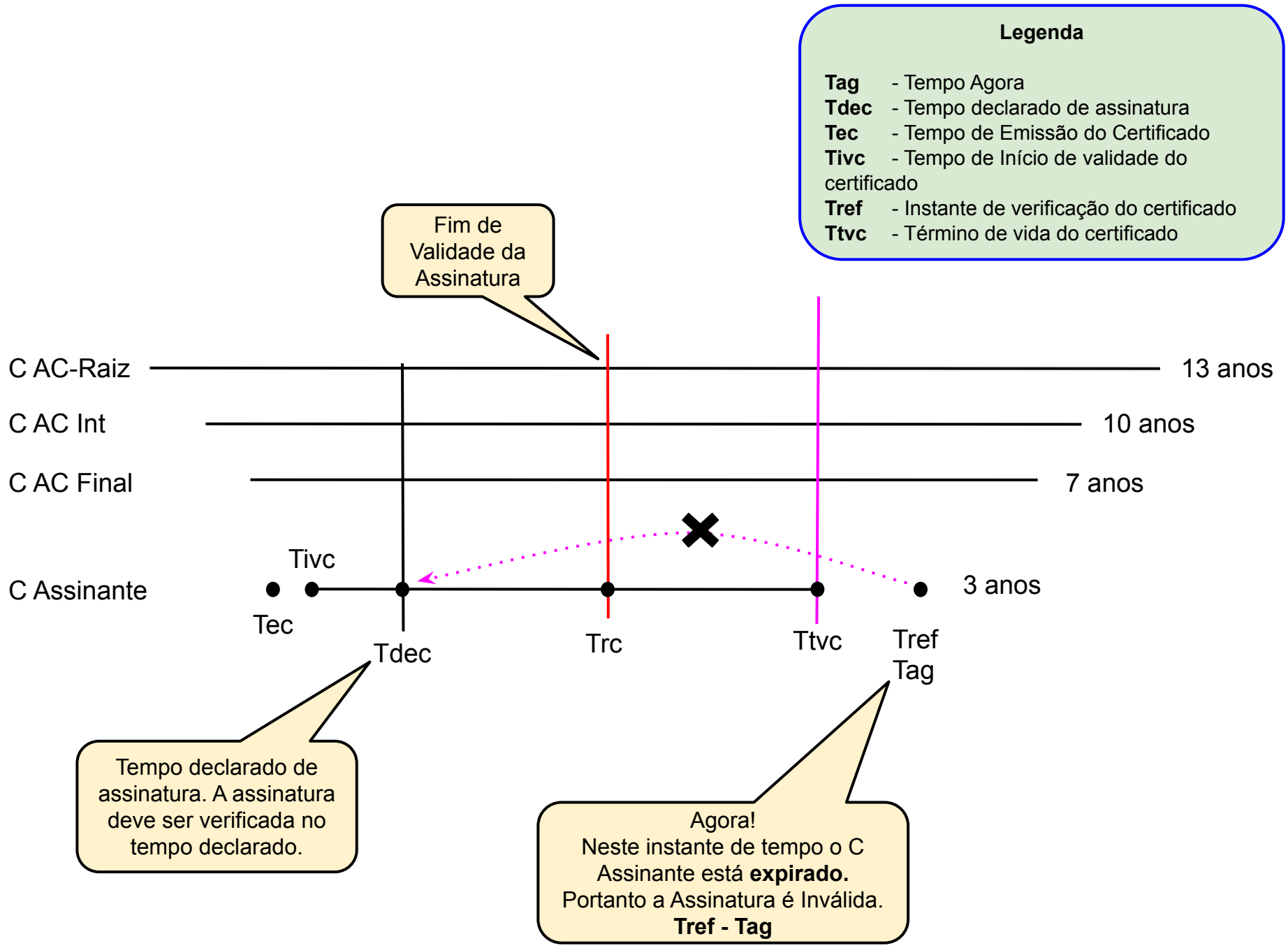

AC Raiz
Offline
AC
Serpro
AR
Requisição de
Certificado
AC
Serpro Final
Online
Instalação Técnica
AR
e-CPF
Receita Federal
Cartão Criptográfico Pronova
Beto
Assinador
Hash
Documento
Ass
PIN


ON
OBSERVATÓRIO NACIONAL
AC Raiz Brasileira
ITI
Sistema de Auditoria e Sincronismo
Hora Legal Brasileira (HLB)
SCT
Autoridade de Carimbo do Tempo (ACT)
RFC 3161
Cliente
Assinador


Legenda
Tag - Tempo Agora
Tdec - Tempo declarado de assinatura
Tec - Tempo de Emissão do Certificado
Tivc - Tempo de Início de validade do certificado
Tref - Instante de verificação do certificado
Ttvc - Término de vida do certificado
Fim de Validade da Assinatura
C AC-Raiz
13 anos
C AC Int
10 anos
C AC Final
7 anos
C Assinante
3 anos
Tivc
Tec
Tdec
Tref
Tag
Ttvc
Tempo declarado de assinatura. A assinatura deve ser verificada no tempo declarado.
Agora!
Neste instante de tempo o C Assinante está válido.
A assinatura é válida.
Tref = Tag


Legenda
Tag - Tempo Agora
Tdec - Tempo declarado de assinatura
Tec - Tempo de Emissão do Certificado
Tivc - Tempo de Início de validade do certificado
Tref - Instante de verificação do certificado
Ttvc - Término de vida do certificado
Fim de Validade da Assinatura
C AC-Raiz
13 anos
C AC Int
10 anos
C AC Final
7 anos
C Assinante
3 anos
Tivc
Tec
Tdec
Ttvc
Tref
Tag
Tempo declarado de assinatura. A assinatura deve ser verificada no tempo declarado.
Agora!
Neste instante de tempo o C Assinante está expirado.
Portanto a assinatura não é válida.
Tref = Tag


Legenda
Tag - Tempo Agora
Tdec - Tempo declarado de assinatura
Tec - Tempo de Emissão do Certificado
Tivc - Tempo de Início de validade do certificado
Tref - Instante de verificação do certificado
Ttvc - Término de vida do certificado
Fim de Validade da Assinatura
C AC-Raiz
13 anos
C AC Int
10 anos
C AC Final
7 anos
C Assinante
3 anos
Tivc
Tec
Tdec
Trc
Tref
Tag
Ttvc
Tempo declarado de assinatura. A assinatura deve ser verificada no tempo declarado.
Agora!
Neste instante de tempo o C Assinante está **revogado.**
Portanto a Assinatura é Inválida.
Tref - Tag


Legenda
Tag - Tempo Agora
Tdec - Tempo declarado de assinatura
Tec - Tempo de Emissão do Certificado
Tivc - Tempo de Início de validade do certificado
Tref - Instante de verificação do certificado
Ttvc - Término de vida do certificado
Fim de Validade da Assinatura
C AC-Raiz
13 anos
C AC Int
10 anos
C AC Final
7 anos
C Assinante
3 anos
Tivc
Tec
Tdec
Trc
Ttvc
Tref
Tag
Tempo declarado de assinatura. A assinatura deve ser verificada no tempo declarado.
Agora!
Neste instante de tempo o C Assinante está expirado.
Portanto a Assinatura é Inválida.
Tref - Tag

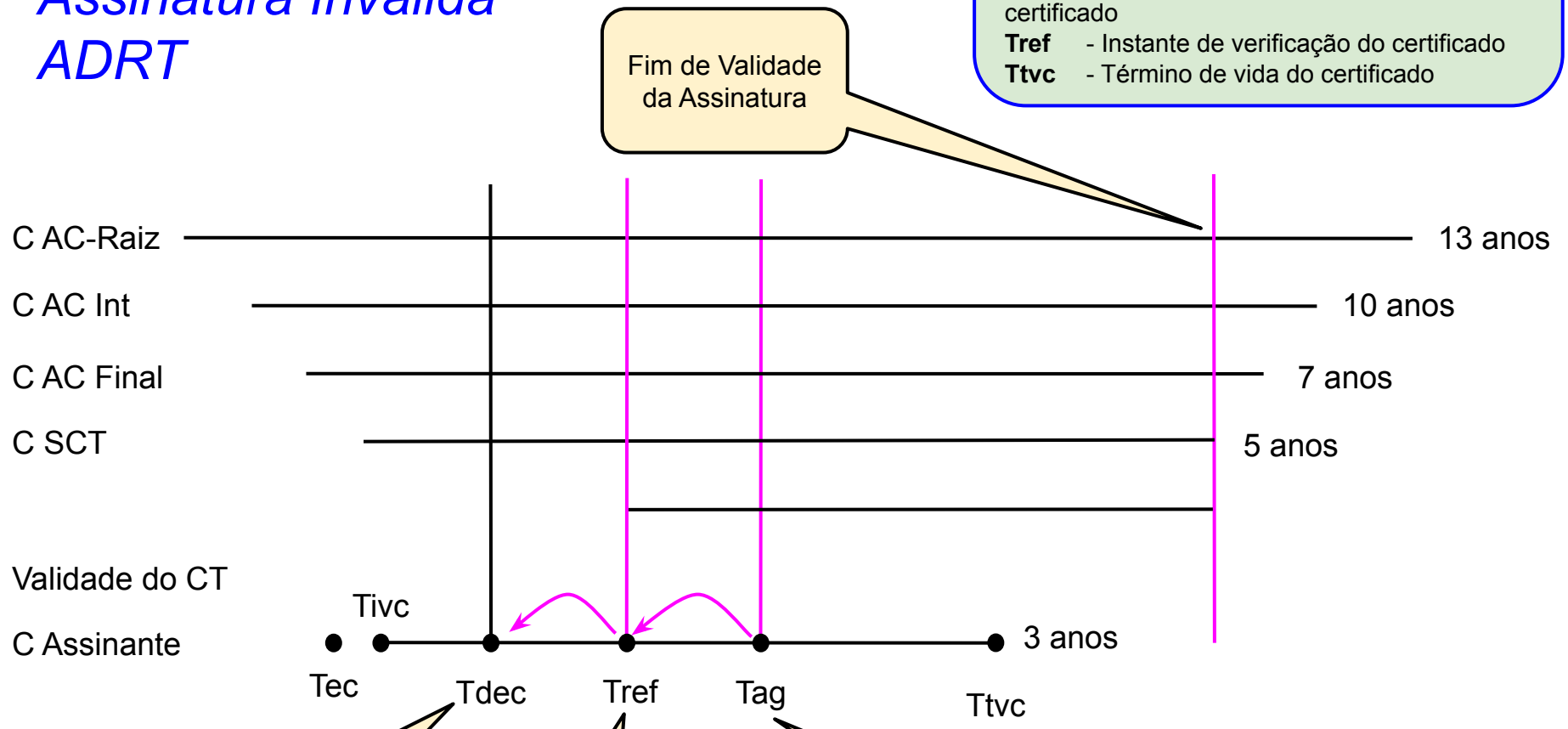
Ciclo de Vida

Assinatura Inválida

ADRT

Legenda

Tag - Tempo Agora
Tdec - Tempo declarado de assinatura
Tec - Tempo de Emissão do Certificado
Tivc - Tempo de Início de validade do certificado
Tref - Instante de verificação do certificado
Ttvc - Término de vida do certificado

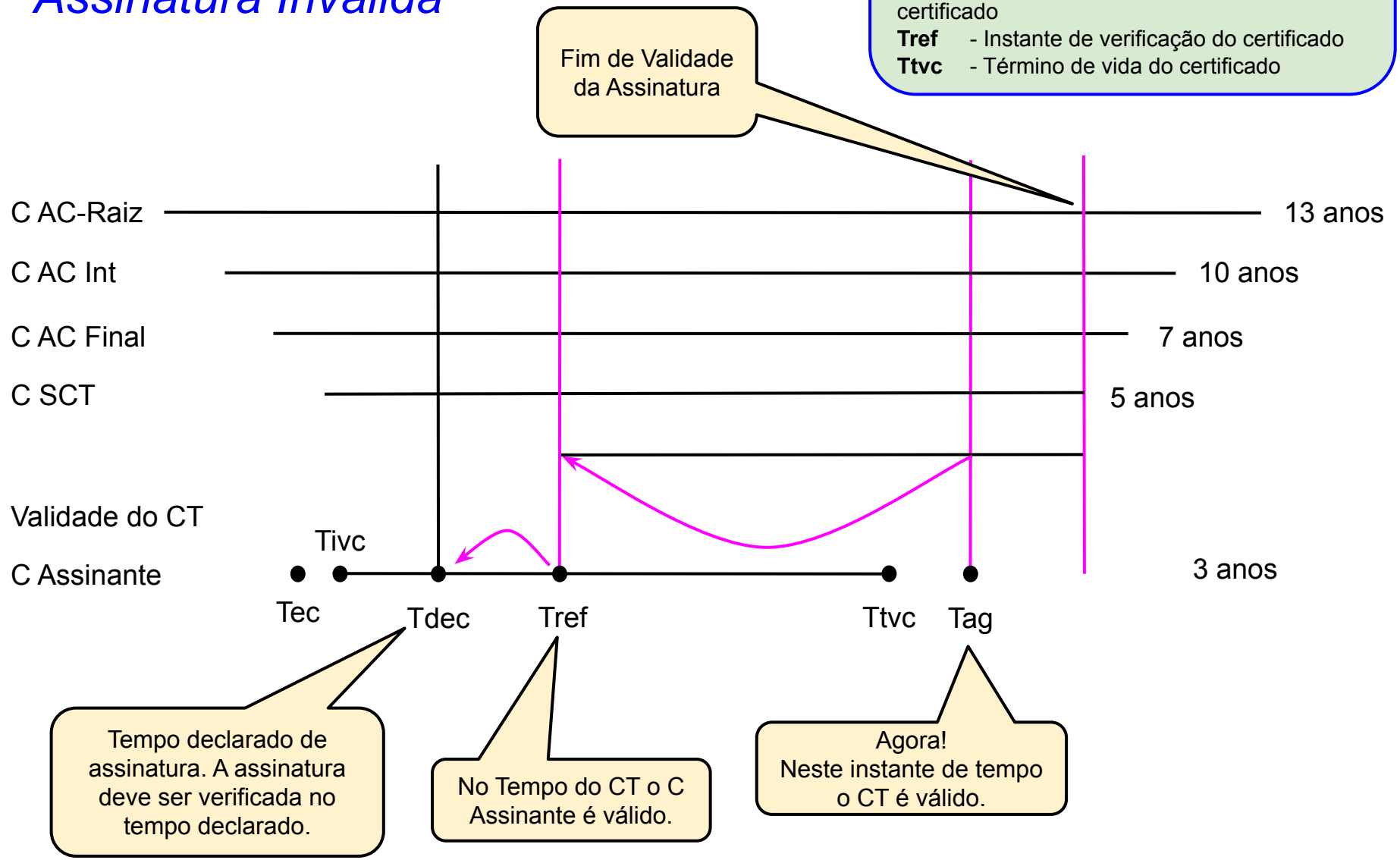


Ciclo de Vida

Assinatura Inválida

Legenda

Tag - Tempo Agora
Tdec - Tempo declarado de assinatura
Tec - Tempo de Emissão do Certificado
Tivc - Tempo de Início de validade do certificado
Tref - Instante de verificação do certificado
Ttvc - Término de vida do certificado

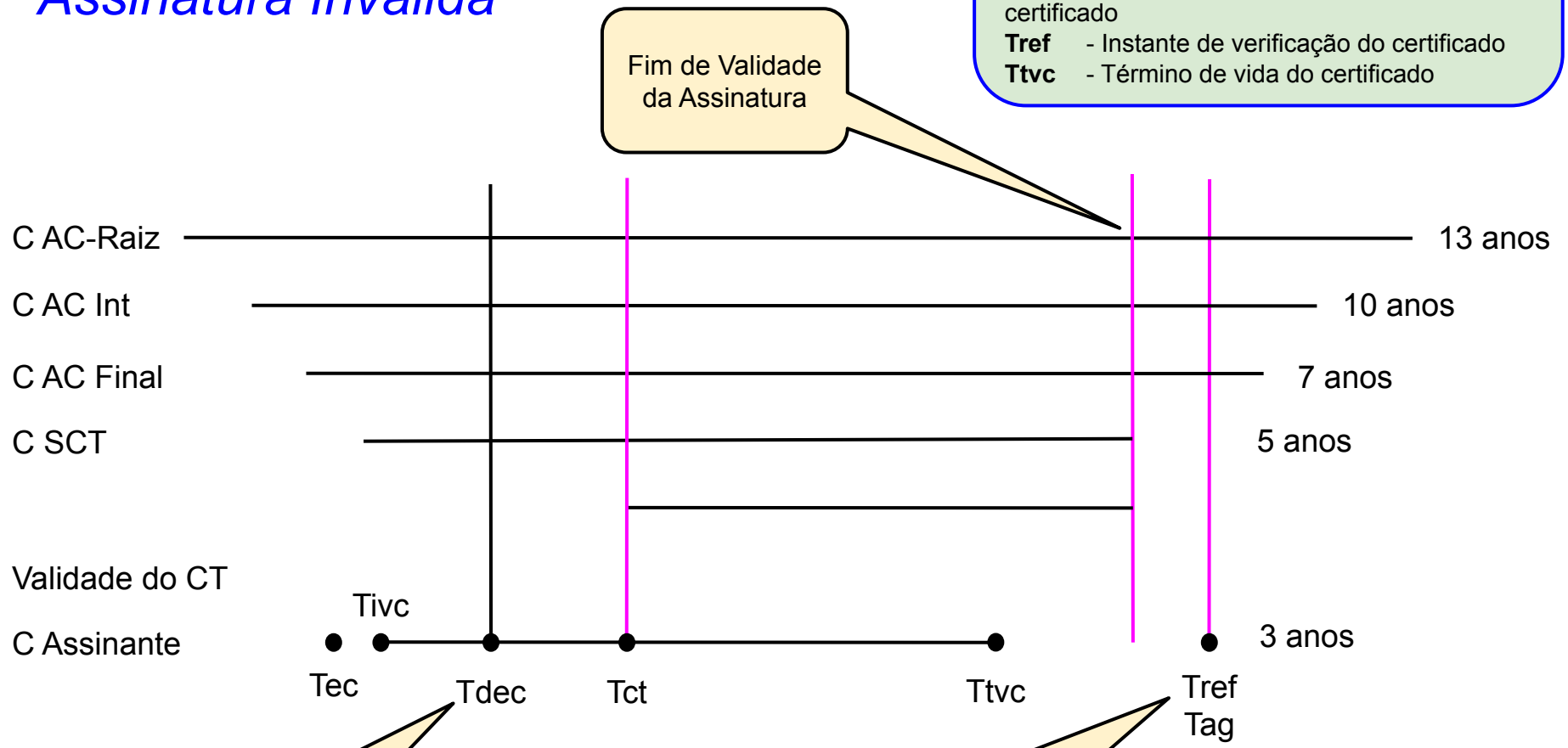


Ciclo de Vida

Assinatura Inválida

Legenda

Tag - Tempo Agora
Tdec - Tempo declarado de assinatura
Tec - Tempo de Emissão do Certificado
Tivc - Tempo de Início de validade do certificado
Tref - Instante de verificação do certificado
Ttvc - Término de vida do certificado

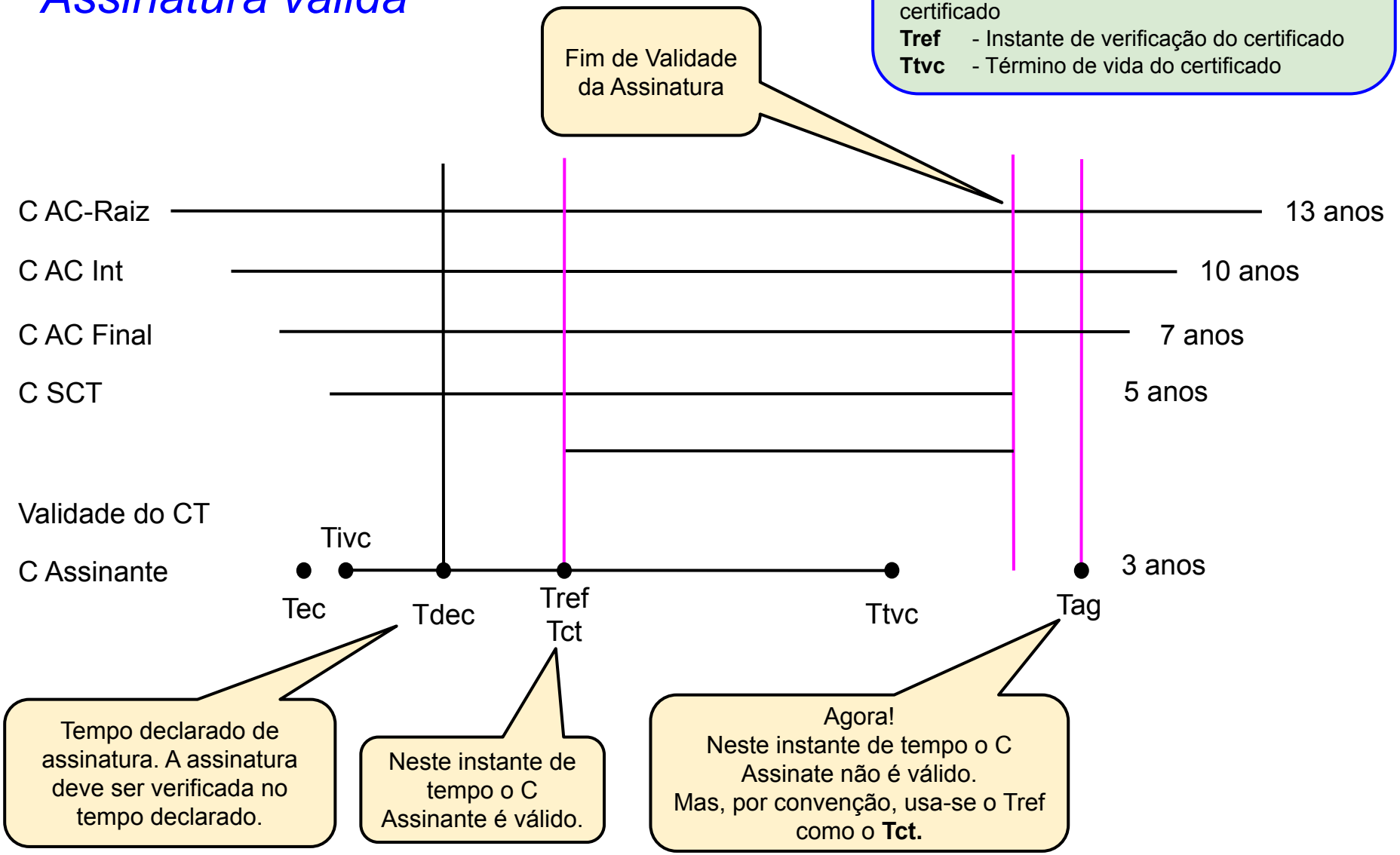


Ciclo de Vida

Assinatura válida

Legenda

Tag - Tempo Agora
Tdec - Tempo declarado de assinatura
Tec - Tempo de Emissão do Certificado
Tivc - Tempo de Início de validade do certificado
Tref - Instante de verificação do certificado
Ttvc - Término de vida do certificado



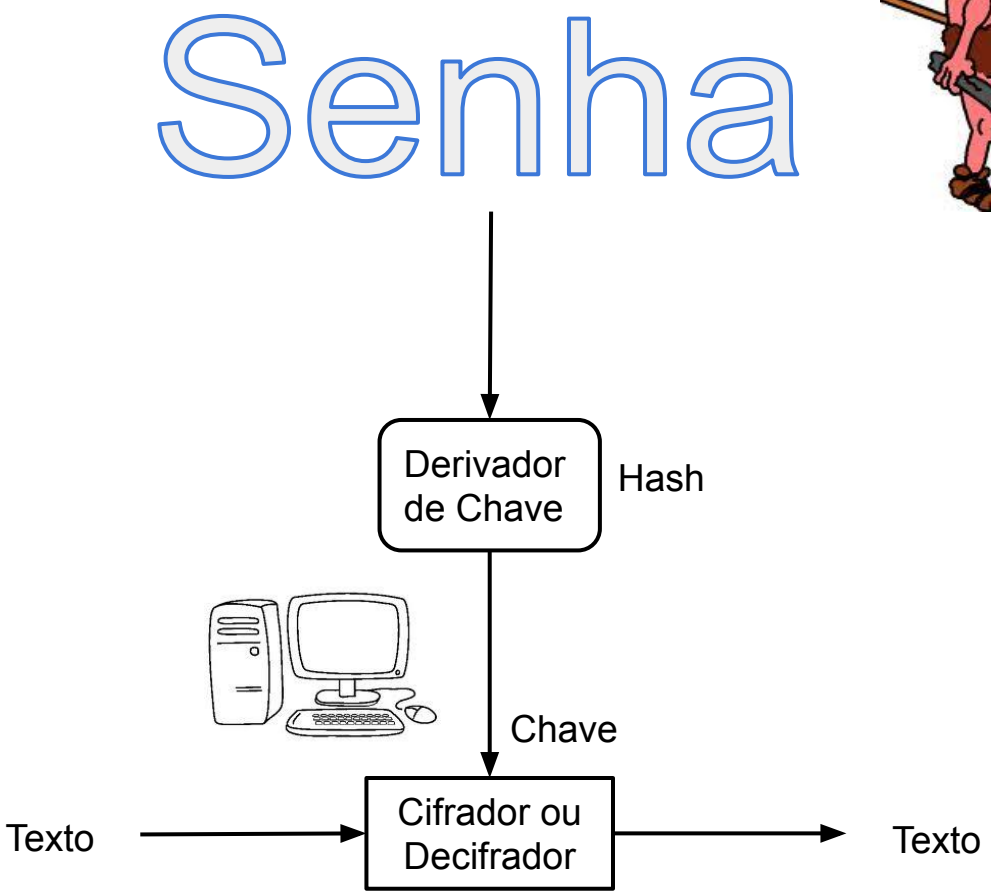
Princípios das Chaves de Assinatura

- Unicidade
- Uma única cópia
  - Não há a necessidade de cópias
  - Poucas situações onde a cópia é desejável
- Revogação
- Chave de Assinatura deve ser destruída quando não for mais necessária
  - Carimbo do Tempo

Tamanho das Chaves

- Simétrica
  - 40, 56, 64, **128**, 192, 256 bits
  - Ex: Blowfish, CAST, DES, Gost, IDEA, RC2, RC4, RC5, AES
- Assimétrica
  - RSA
    - 1024, **2048** ou 4096 bits
  - ECDSA
    - 256 bits
    - Curvas Primas e Curvas Binárias
- Assinatura
  - 512, **1024**, **2048**, 3072 ou 4096 bits
  - DSA - só para assinatura, não para ciframento

Senhas e Chaves



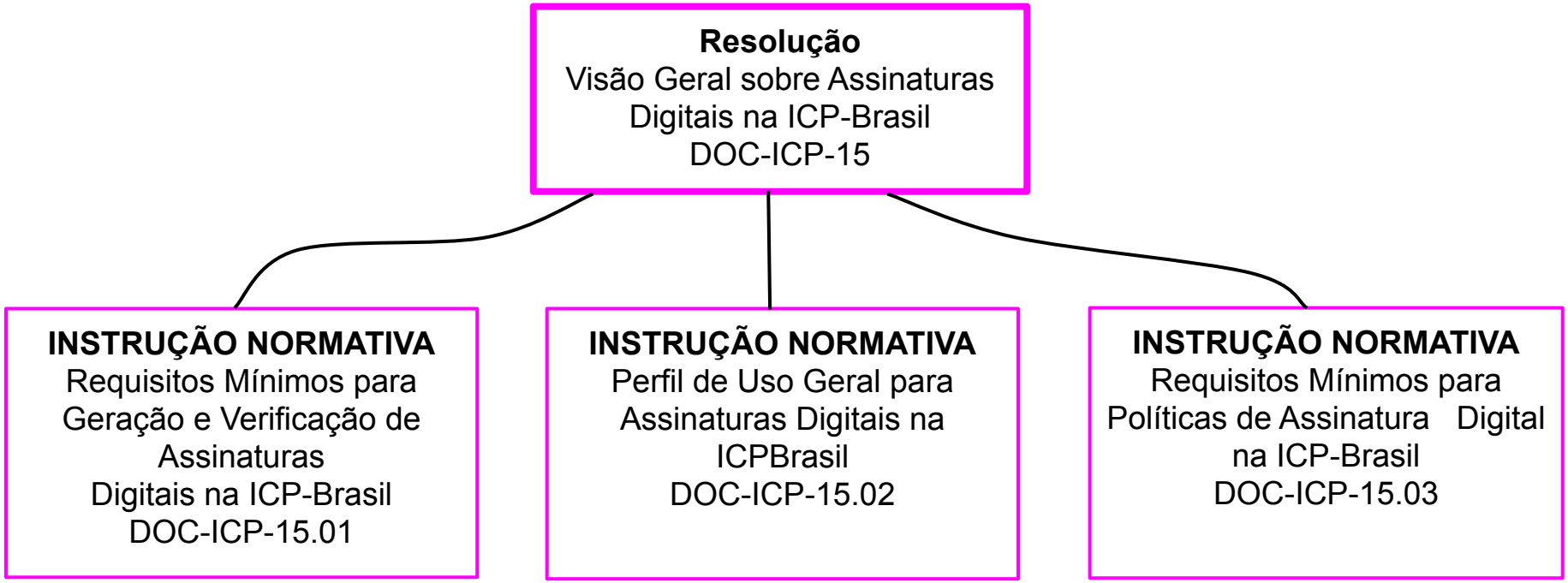
Representação de Mensagens Cifradas

- PKCS #7, CMS, PAdES, CAdES, XAdES
  - Armazena informações adicionais sobre o conteúdo cifrado (ex: algorítmo utilizado, informações de quem realizou o ciframento/assinatura, etc)

- Base64, PEM, DER
  - Armazena qualquer tipo de informação, desde apenas o conteúdo cifrado, até estruturas de dados mais complexas, como os valores codificados dos formatos apresentados acima.

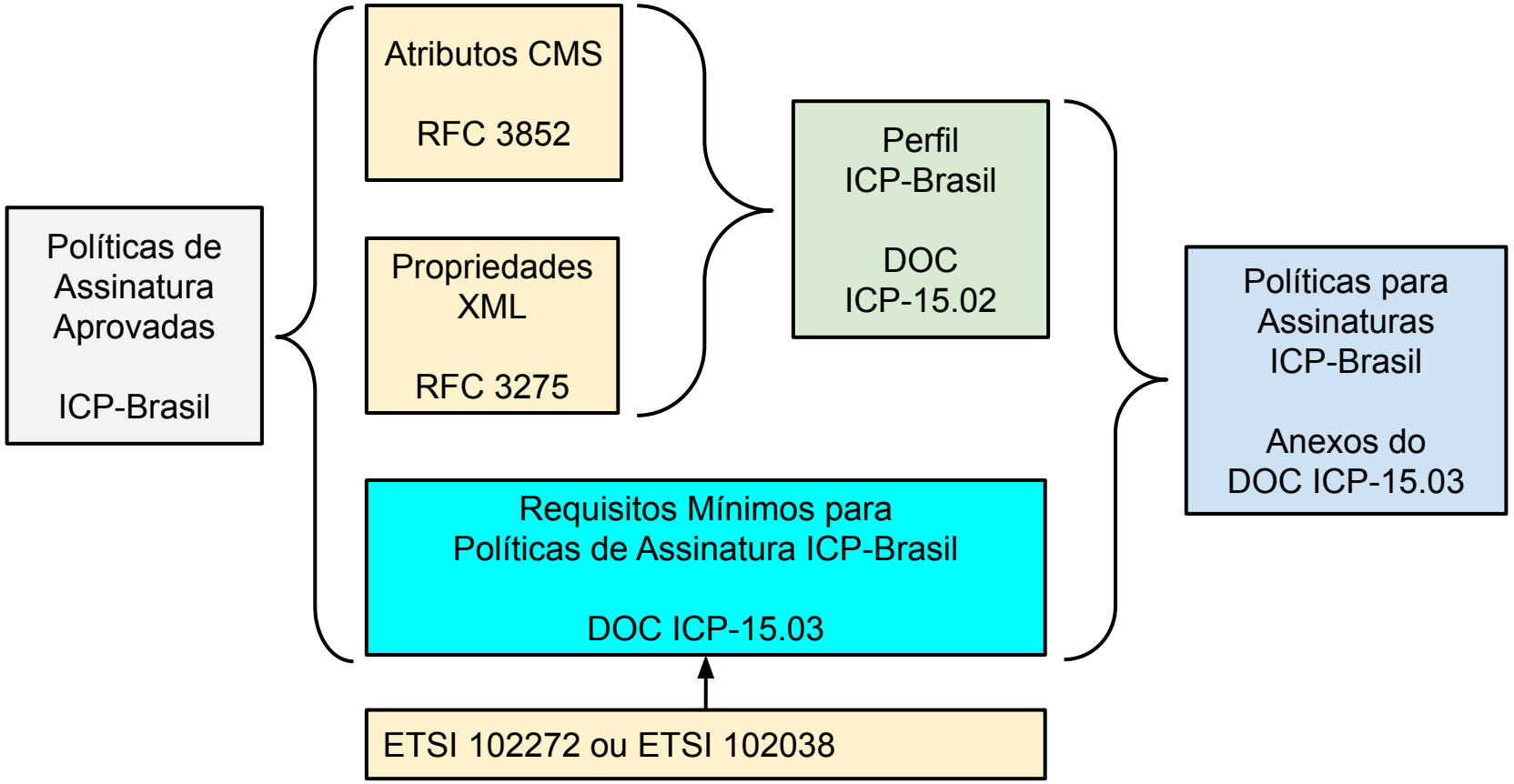
Padrão Brasileiro de Assinatura Digital

Âmbito da ICP-Brasil

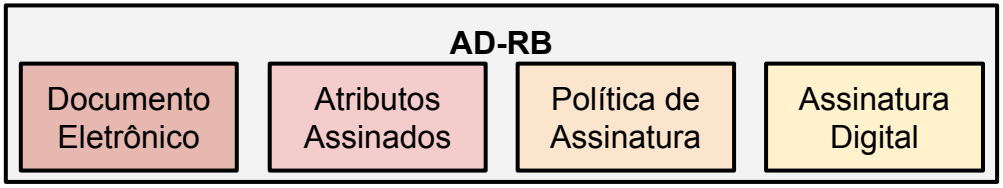


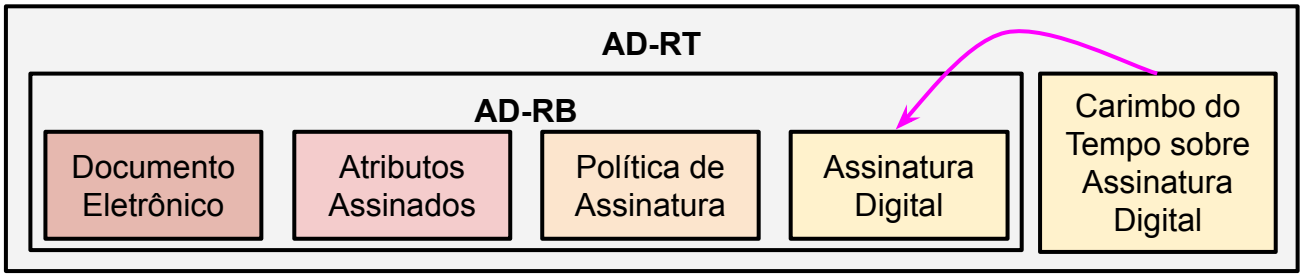
Marco Regulatório

Carimbo do Tempo

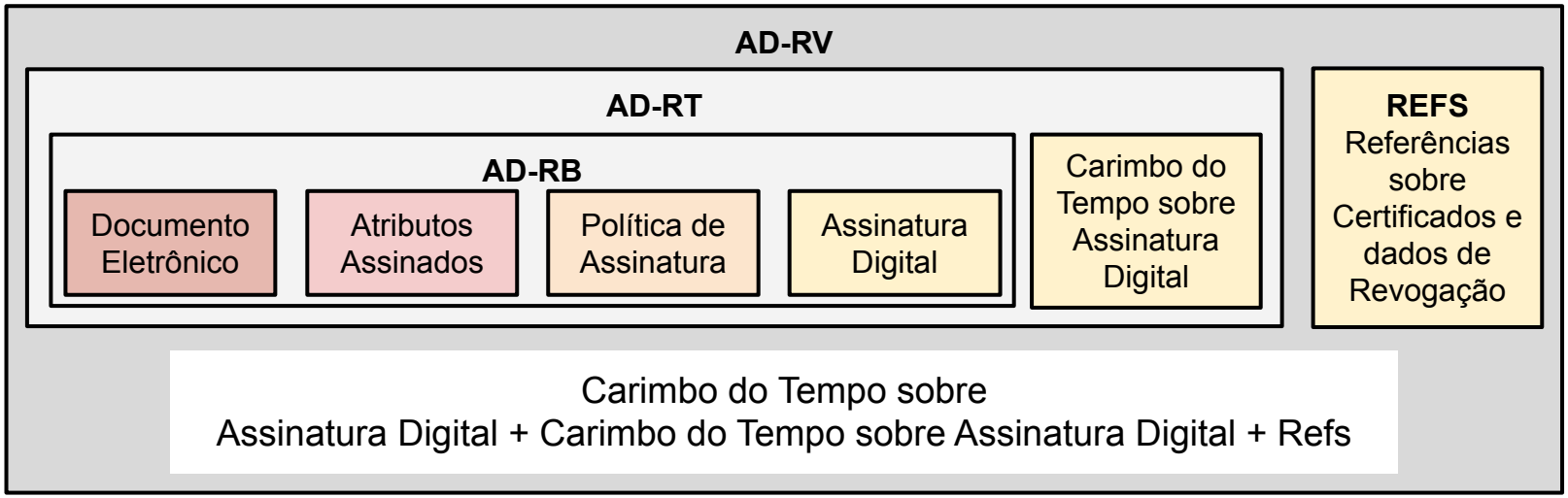


Assinatura Digital com Referência Básica e de Tempo

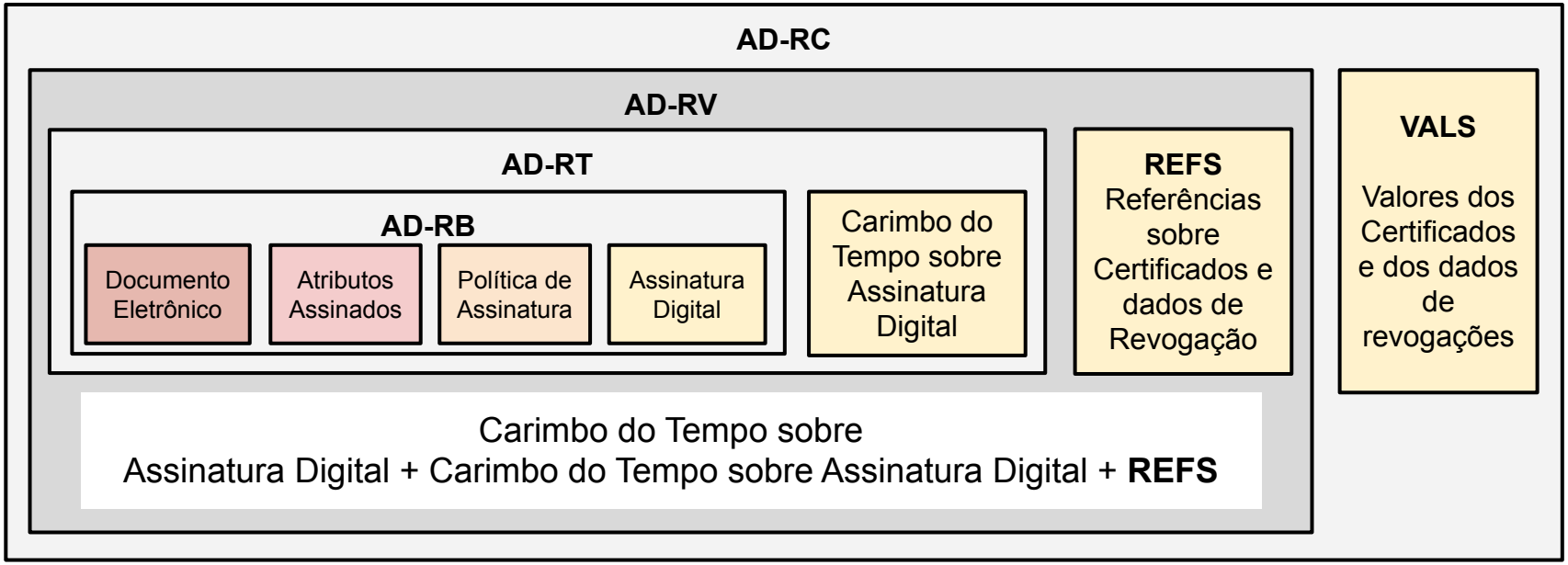




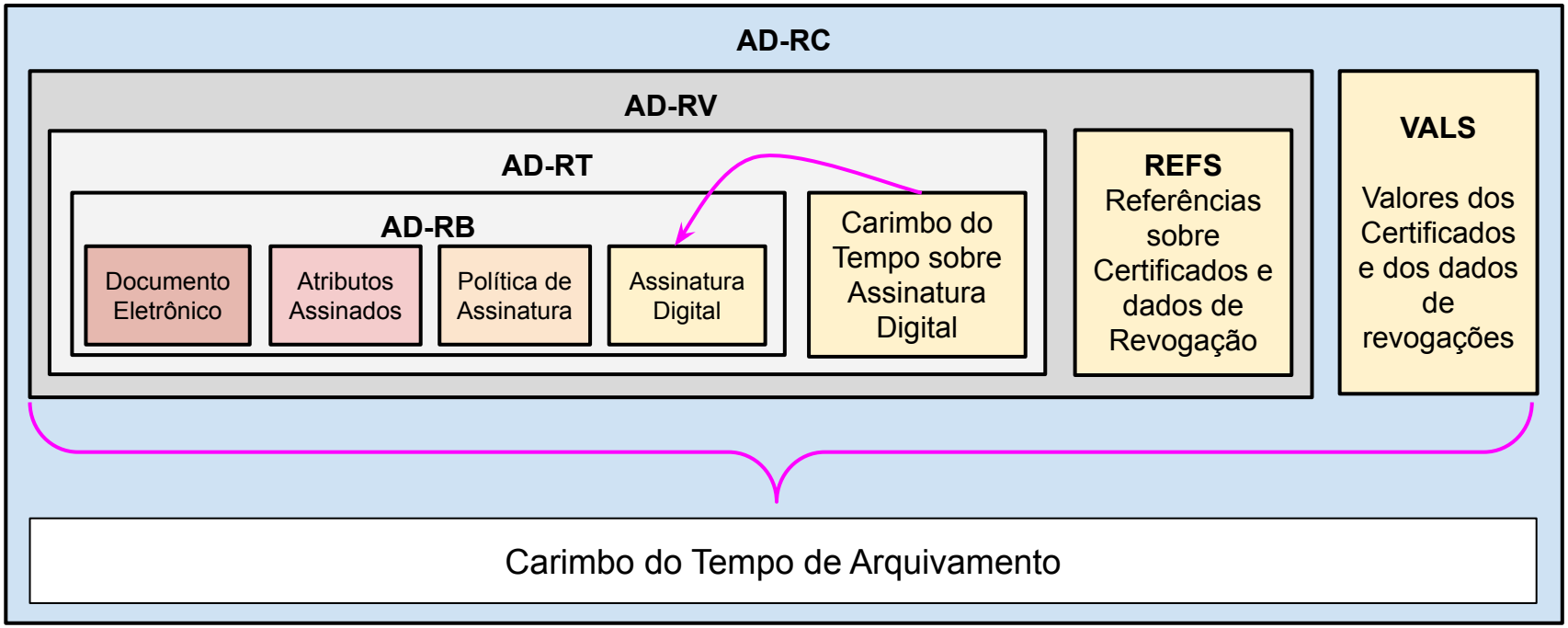
Assinatura Digital com Referências para Validação



Assinatura Digital com Referências Completas



Assinatura Digital com Referências para Arquivamento



Certificados de Atributos

Certificado de Atributo (CA)

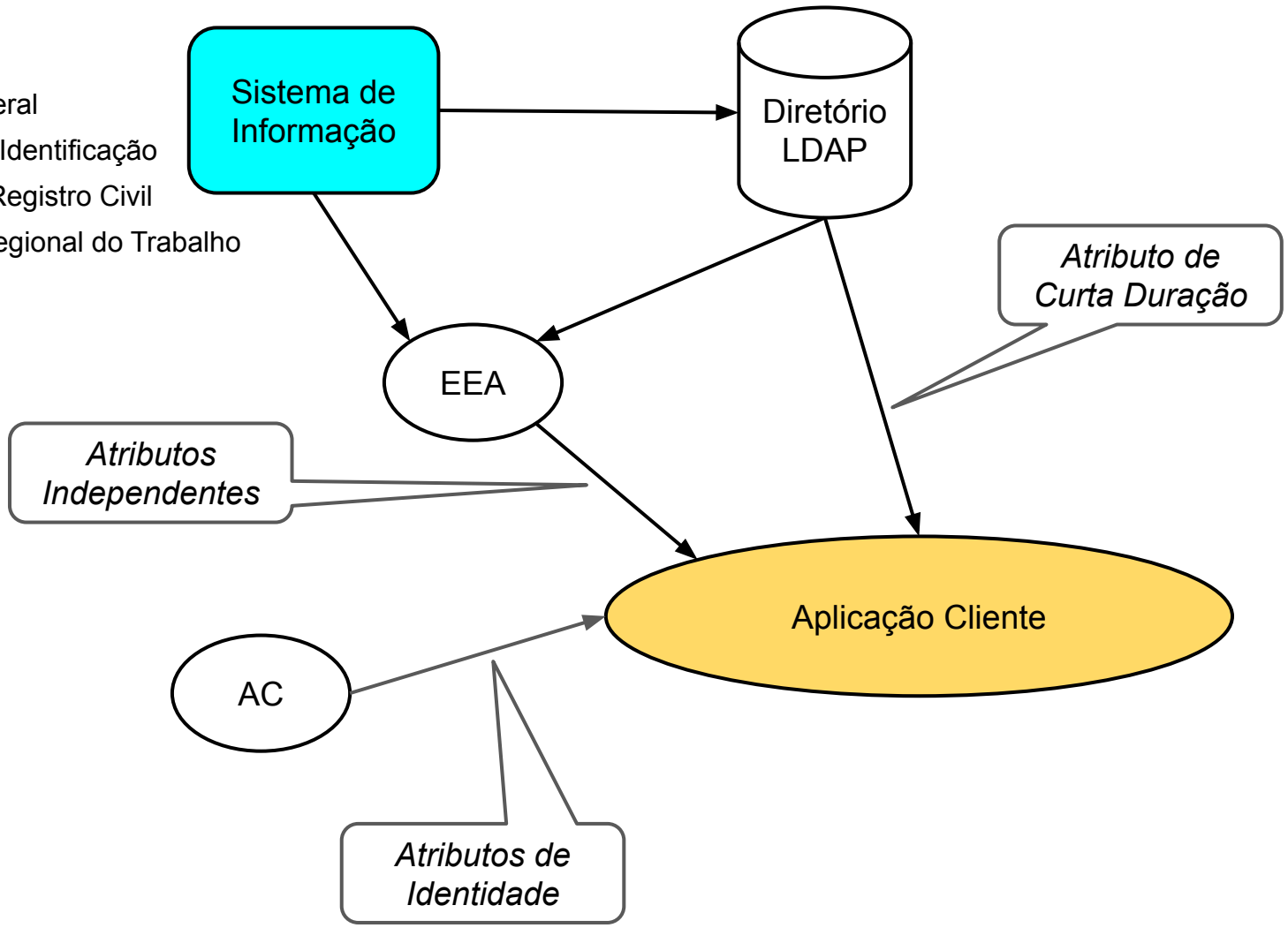
Número da Versão
Número Serial
Algoritmo de Assinatura
Emissor
Período de Validade
Titular
Atributos
Identificador Único do Emissor
Extensões
Assinatura da ACA

Certificado Digital (CI)

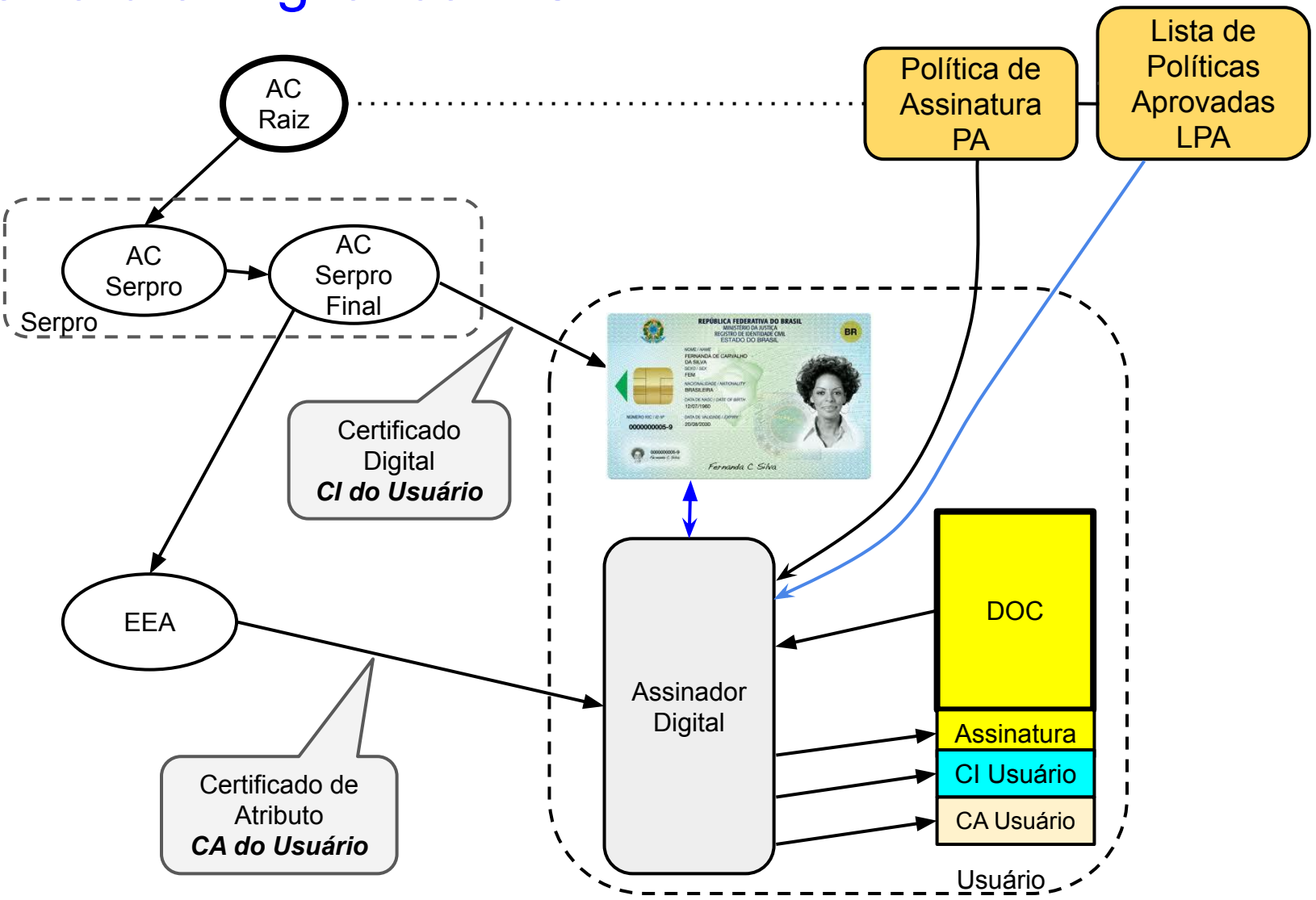
Número da Versão
Número Serial
Algoritmo de Assinatura
Emissor
Período de Validade
Sujeito
Algoritmo de Chave Pública
Chave Pública
Identificador Único do Emissor
Identificador Único do Sujeito
Extensões
Assinatura da AC

Fontes de Atributos

DETRAN
TRE
Receita Federal
Institutos de Identificação
Cartório de Registro Civil
Delegacia Regional do Trabalho



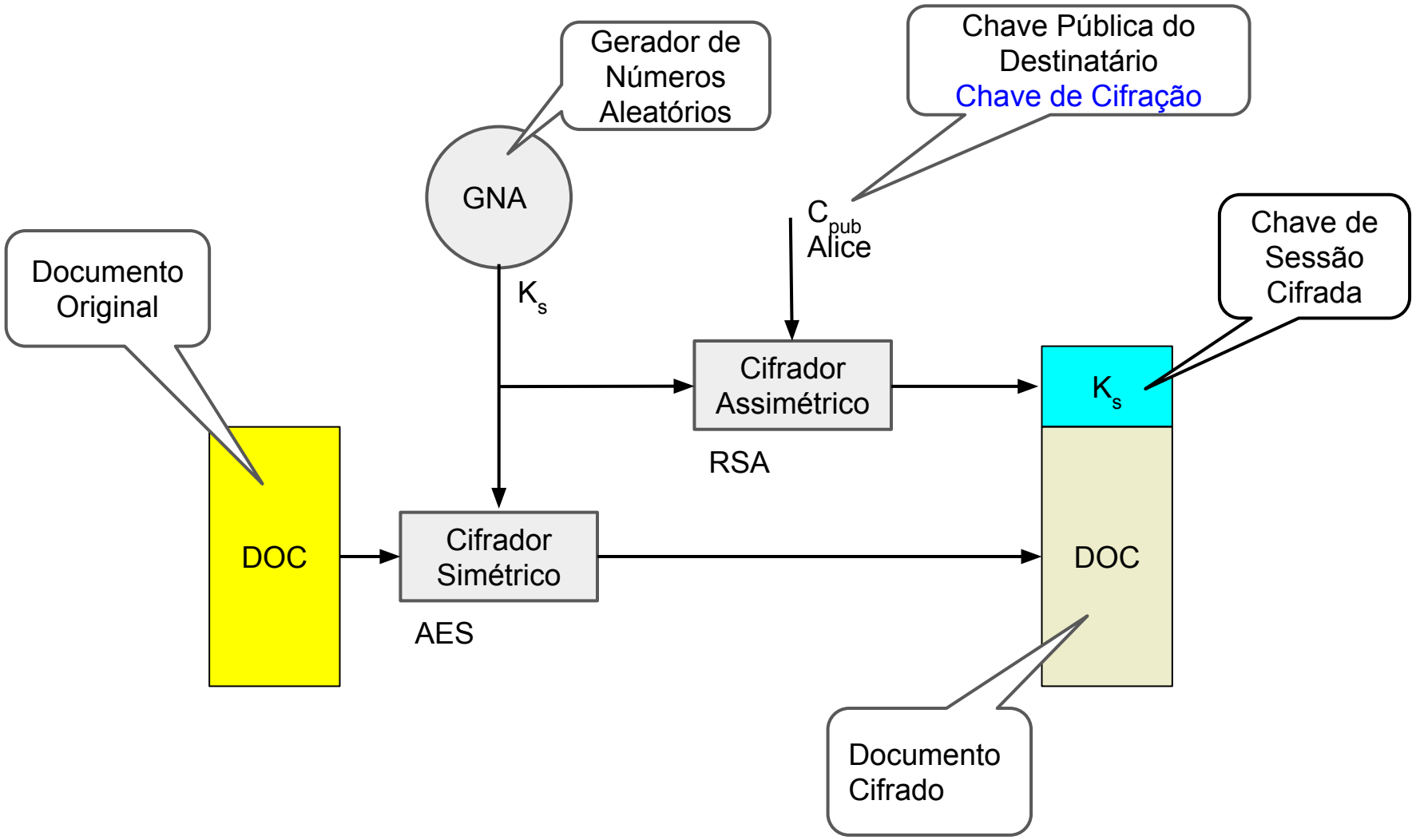
Assinatura Digital com CA



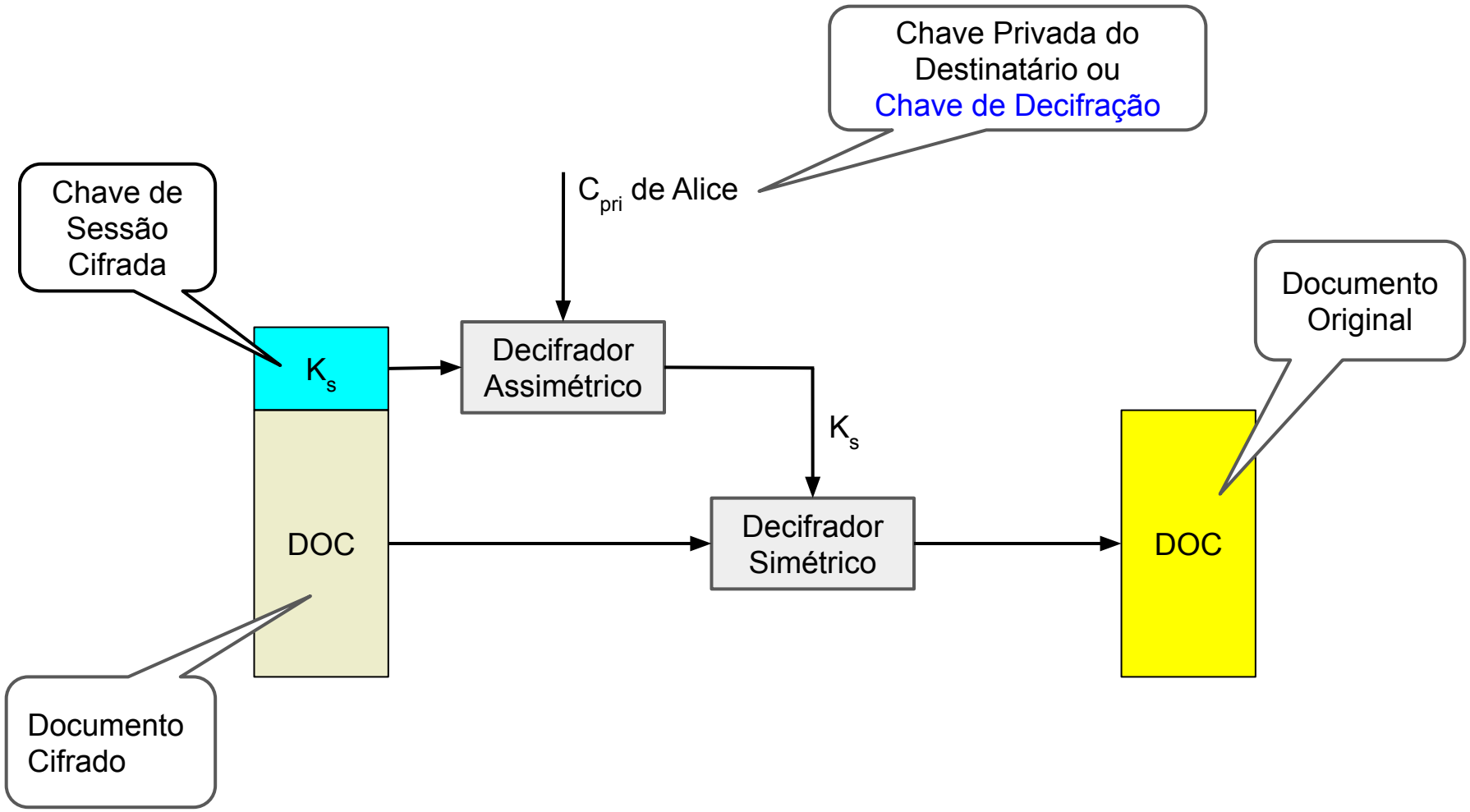
Aplicações de Certificação Digital

- Site Seguro (SSL, WTLS)
- E-mail Seguro
  - Assinatura Digital
  - Sigilo
- Assinatura de Documentos
  - PDF, OpenXML, Open Document File
- IPSec
- VPN
- Autenticação

Ciframento de Documentos Eletrônicos - Sigilo



Uso de Chaves de Sessão para Deciframento



Preservação em Longo Prazo

Assinaturas Digitais

- Terceira Parte
- Uso de Carimbos do Tempo
- Substituição de Algorítmos
- Dispersão por Criptografia de Limiar

Provedores de Serviços Criptográficos

- Sistemas Operacionais
  - Windows
    - CryptoAPI
  - Linux / Mac OS X
    - OpenSSL
  - Mac OS X
    - AppleCSP
- Linguagens e Sistemas
  - Java Crypto API
  - PDF Adobe
  - ODF
  - OpenXML