

Agenda

- ✓ Criptografia e Segurança
- ✓ Certificado Digital
- ✓ Assinatura Digital

CRIPTOGRAFIA E SEGURANÇA

Criptografia e Segurança

- Necessidade de proteção da privacidade
- Problema de login-senha
- Autenticação multifatores
- Algoritmos de Hash
- Chaves simétricas e assimétricas
- Criptografia usa problemas matemáticos difíceis de resolver (PLD e Fatoração)
- Permitem assegurar confidencialidade, autenticidade, integridade e não-repúdio

SECURING YOURSELF FROM A WORLD OF HACKERS:



How to avoid the most common and dangerous passwords

In a recent survey conducted by ZoneAlarm, 79% of consumers were found to use risky password construction practices, such as using personal information and common words. Here are examples of these in order from the number one most commonly used password of all time.

THE TOP 20 PASSWORDS OF ALL TIME

1	123456	11	Nicole
2	12345	12	Daniel
3	123456789	13	babygirl
4	Password	14	monkey
5	iloveyou	15	Jessica
6	princess	16	Lovely
7	rockyou	17	michael
8	1234567	18	Ashley
9	12345678	19	654321
10	abc123	20	Qwerty

4%

Estimated percentage of consumers who use some variant of the word "password."

25%

Proportion of top 20 most commonly used passwords that are first names.

16%

Overall percentage of consumers who create passwords using a person's first name.

Fonte: ZoneAlarm

- Algoritmos utilizados na ICP-Brasil
 - Chaves Públicas
 - RSA (*Rivest, Shamir, Adleman*)
 - ECC (Curvas Elípticas), *ECCBrainpool**
 - Chaves Simétricas
 - 3DES
 - AES
 - Resumo (*Hash*)
 - SHA1
 - SHA256
 - SHA512



INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

CERTIFICADO DIGITAL

Certificado Digital

Como funciona o Certificado Digital?

- Funciona como uma espécie de carteira de identidade virtual que permite a identificação segura do autor de uma mensagem ou transação em rede de computadores;
- Utiliza procedimentos lógicos e matemáticos complexos que permitem assegurar confidencialidade, autenticidade, integridade e irretratabilidade.

Certificado Digital

O que é Certificado Digital?

- É um documento eletrônico, gerado e assinado digitalmente por uma terceira parte confiável (AC), que de acordo com regras estabelecidas associa uma entidade a um par de chaves criptográficas;
- Um certificado digital contém dados do titular, a AC que emitiu e sua assinatura, podendo conter ainda dados complementares.



Certificado Digital

E para que serve o Certificado Digital?

- Cifragem (sigilo ou confidencialidade);
- Autenticação de Clientes e/ou Servidores;
- Assinatura Digital;
- Emissão de carimbo do tempo.



Certificado Digital

DOC-ICP-01.01 – Padrões e Algoritmos Criptográficos da ICP-Brasil

Geração de Chaves Assimétricas de Usuário Final

Normativo ICP-Brasil	DOC-ICP-04 – item 6.1.5.2
Algoritmo	RSA, ECDSA, conforme (RFC 5480)* RFC 5639
Tamanho de chave A1, A2, A3, S1, S2, S3, T3	RSA 1024, RSA 2048, ECDSA 256
Tamanho de chave – A4, S4, T4	RSA 2048, RSA 4096, ECDSA 512



INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

Certificado Digital

DOC-ICP-01.01 – Padrões e Algoritmos Criptográficos da ICP-Brasil

Assinatura de Certificados de Usuário Final

Normativo ICP-Brasil

DOC-ICP-04 – item 7.1.3

Suíte de Assinatura

Sha1WithRSAEncryption
Sha256WithRSAEncryption
Sha256WithECDSAEncryption
Sha512WithRSAEncryption
Sha512WithECDSAEncryption

Certificado Digital

Tipo de certificado	Chave criptográfica			Validade máxima do certificado (anos)
	Tamanho (bits)	Processo de geração	Mídia armazenadora	
A1 e S1	2048	Software	Arquivo PKCS#12	1
A2 e S2	2048	Software	<i>Smart card</i> ou <i>Token</i> , sem capacidade de geração de chave	2
A3 e S3 T3	2048	Hardware	<i>Smart card</i> ou <i>Token</i> , com capacidade de geração de chave T3 em Hardware criptográfico	5
A4 e S4 T4	4096	Hardware	Hardware criptográfico	6 11* (EC)

Certificado Digital

Exemplo de Certificado Digital

Certificado

Geral Detalhes Caminho de certificação

 **Informações sobre o certificado**

Este certificado destina-se ao(s) seguinte(s) fim(ns):

- Prova a sua identidade para um computador remoto
- Protege emails

* Veja a declaração da autoridade de certificação para obter detalhes

Emitido para: NOME DO TITULAR: 99999999999

Emitido por: AC SERASA SRF

Válido a partir de 21/12/2005 **até** 21/12/2007

 Tem uma chave particular correspondente a este certificado.

Declaração do emissor

OK

Certificado

Geral Detalhes Caminho de certificação

Caminho de certificação

-  Autoridade Certificadora Raiz Brasileira
 -  Autoridade Certificadora da Secretaria da Receita Federal v1
 -  AC SERASA SRF emitido por Autoridade Certificadora da S
 -  NOME DO TITULAR: 99999999999

< | >

Exibir certificado

Status do certificado:

Este certificado é válido.

OK

Certificado Digital

Armazenamento do Certificado Digital



A3



A4



A1





INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

ASSINATURA DIGITAL

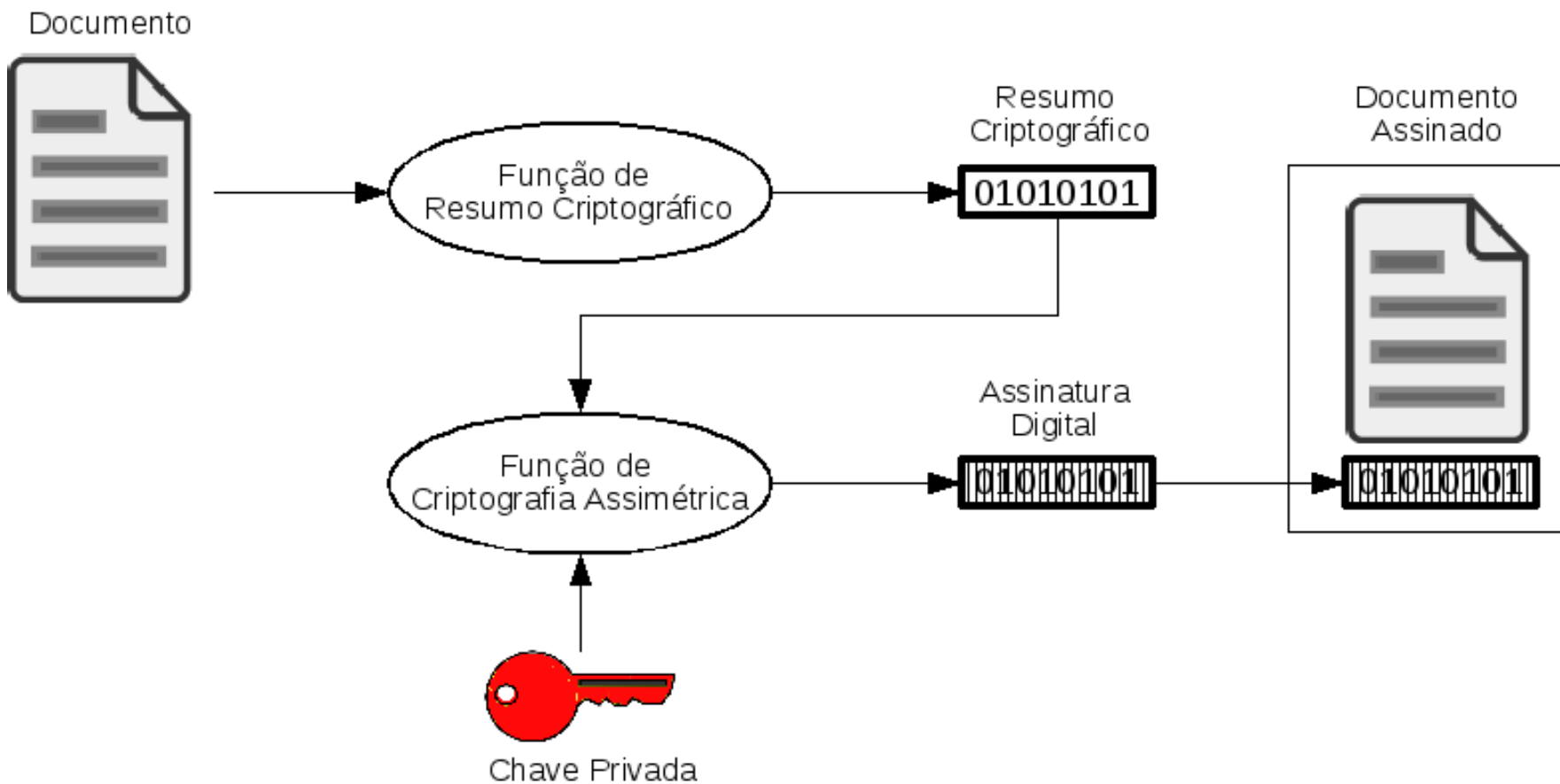
Assinatura Digital

Assinatura Eletrônica

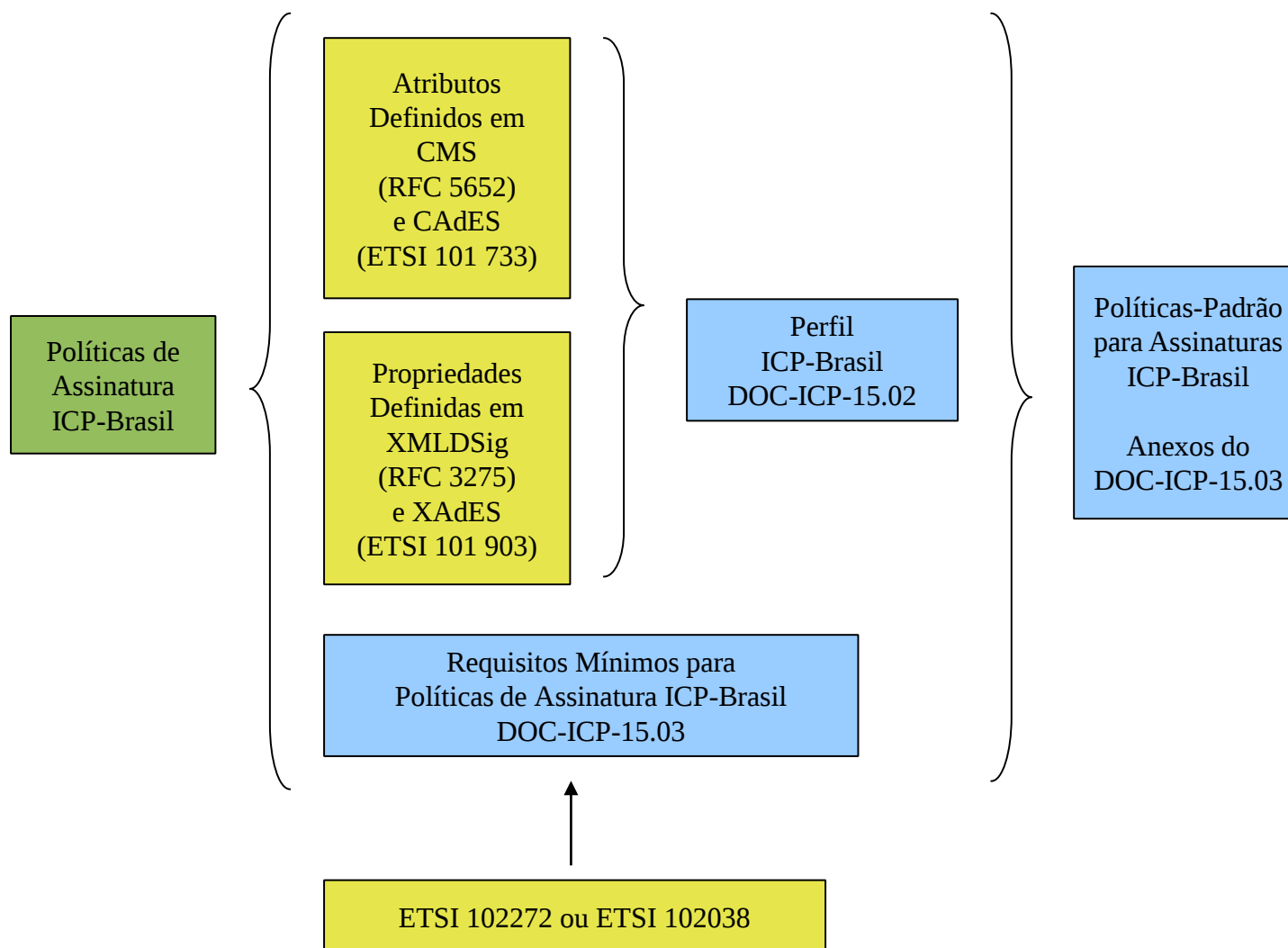
X

Assinatura Digital

Criação de Assinatura Digital



Relação entre Padrões Internacionais e ICP-Br



Assinatura Digital

Ciclo de Vida de uma Assinatura Digital

Processo	Descrição
Criação	Criação de um código logicamente associado a um conteúdo digital e à chave criptográfica privada do signatário.
Verificação ou validação	Verificação quanto à validade de uma ou mais assinaturas digitais logicamente associada a um conteúdo digital.
Armazenamento	Guarda da assinatura digital. Compreende os cuidados para conversão dos dados para mídias mais atuais, sempre que necessário.
Revalidação	Processo que estende a validade do documento assinado, por meio da reassinatura dos documentos ou da aposição de carimbos do tempo, quando da expiração ou revogação dos certificados utilizados para gerar ou revalidar as assinaturas, ou ainda quando do enfraquecimento dos algoritmos criptográficos ou tamanhos de chave utilizados.

Aspectos relevantes

- Preservação do suporte
 - forma
 - conteúdo
 - suporte
- Preservação de longo prazo
 - elementos para preservação
 - fontes, aplicações, etc
 - carimbo do tempo
- Políticas de Assinatura.

Assinatura Digital

AD-B

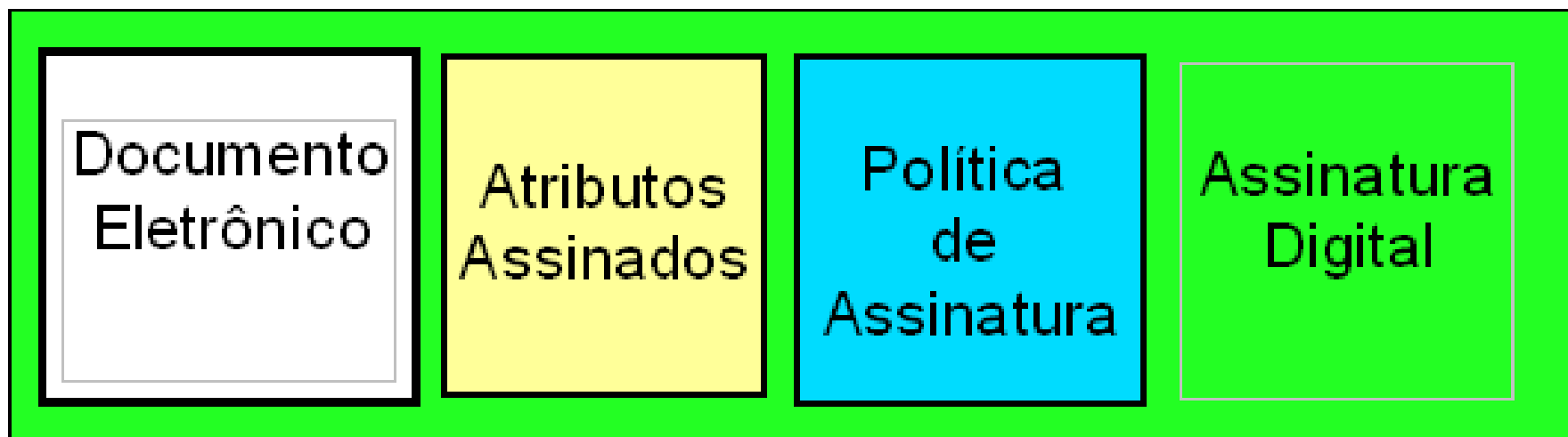


Figura 5a – Assinatura digital básica (AD-B)

Assinatura Digital

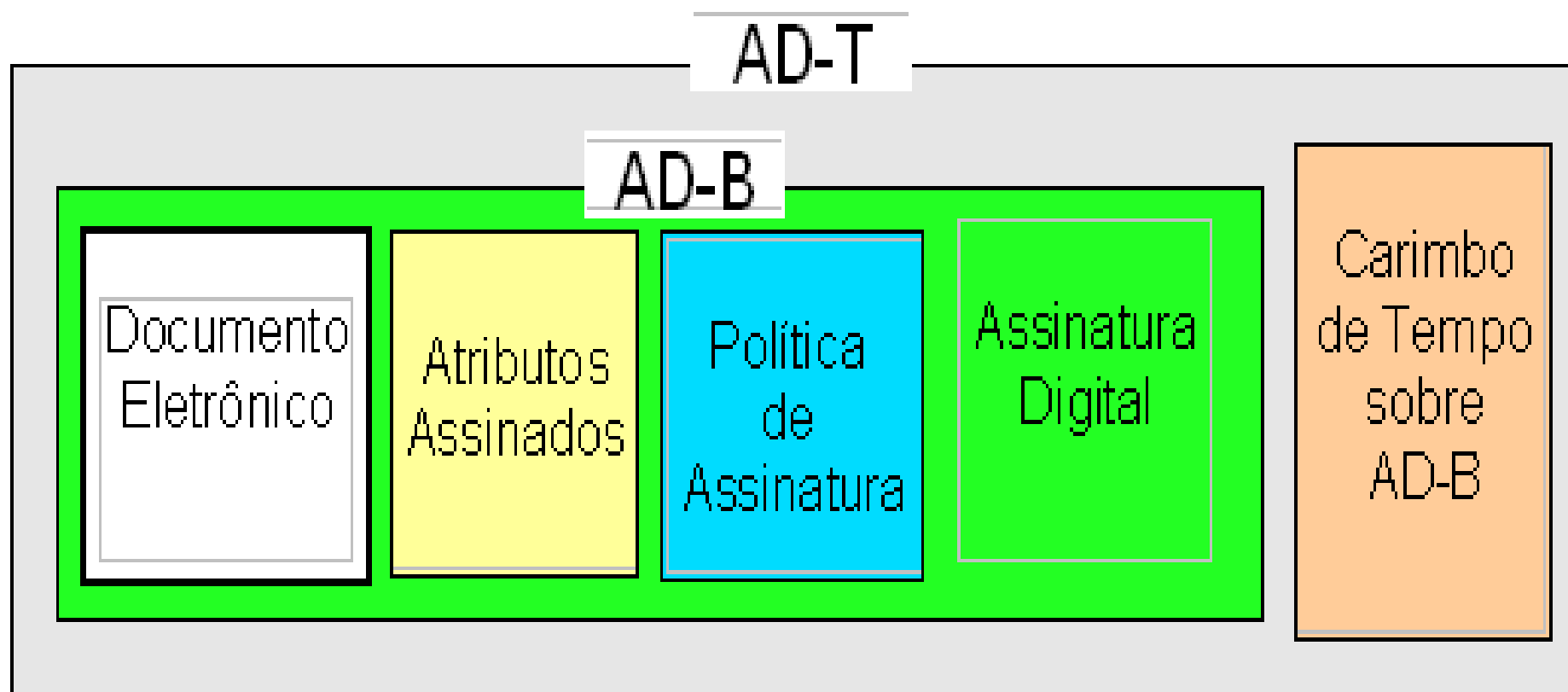


Figura 5b – Assinatura digital com carimbo do tempo (AD-T)

Assinatura Digital

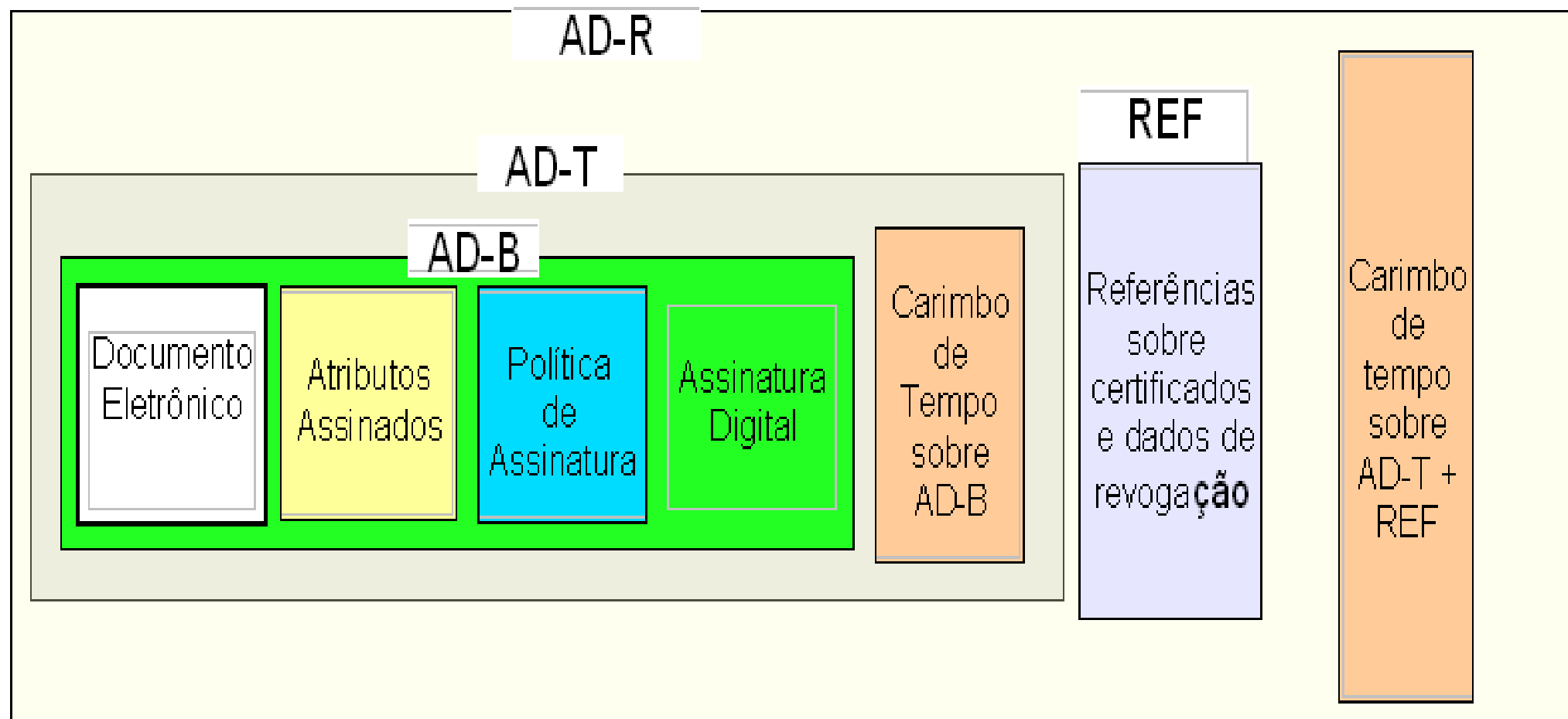


Figura 5c – Assinatura digital com referências para validação (AD-R)

Assinatura Digital

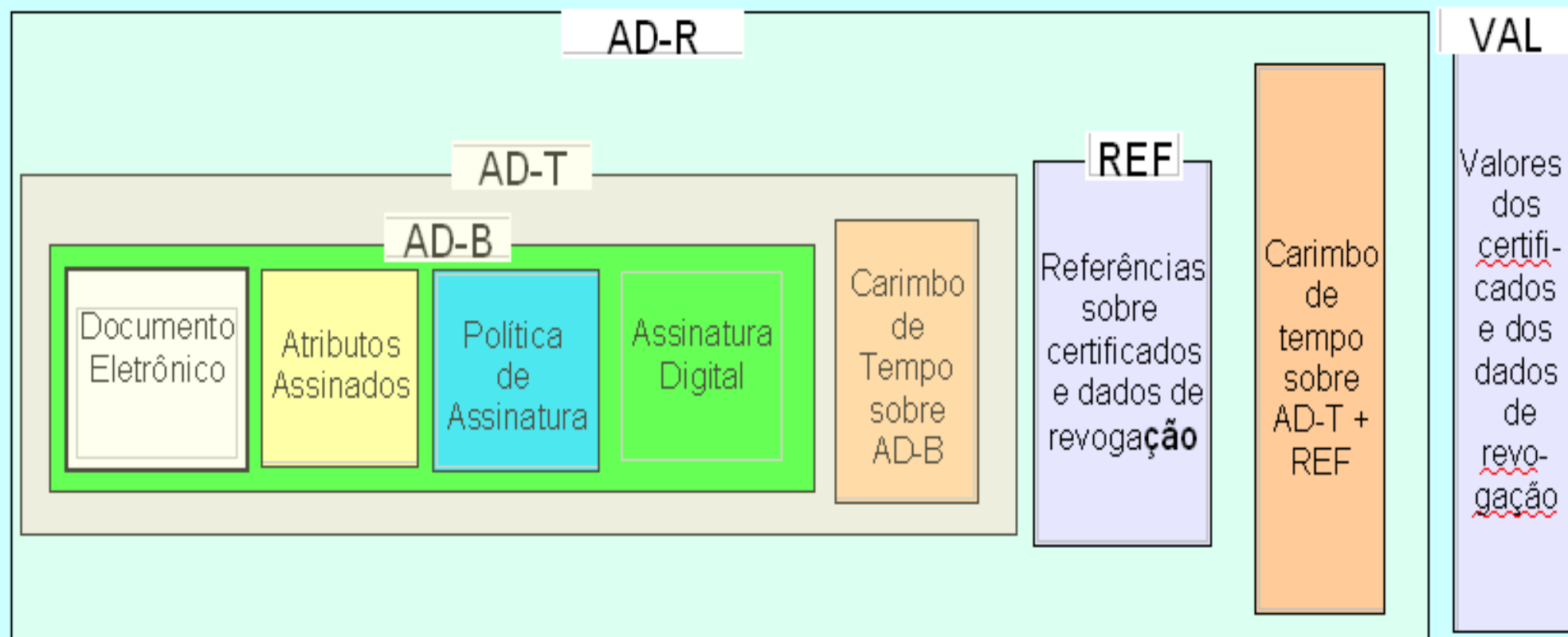


Figura 5d – Assinatura digital com informações completas (AD-C)

Assinatura Digital

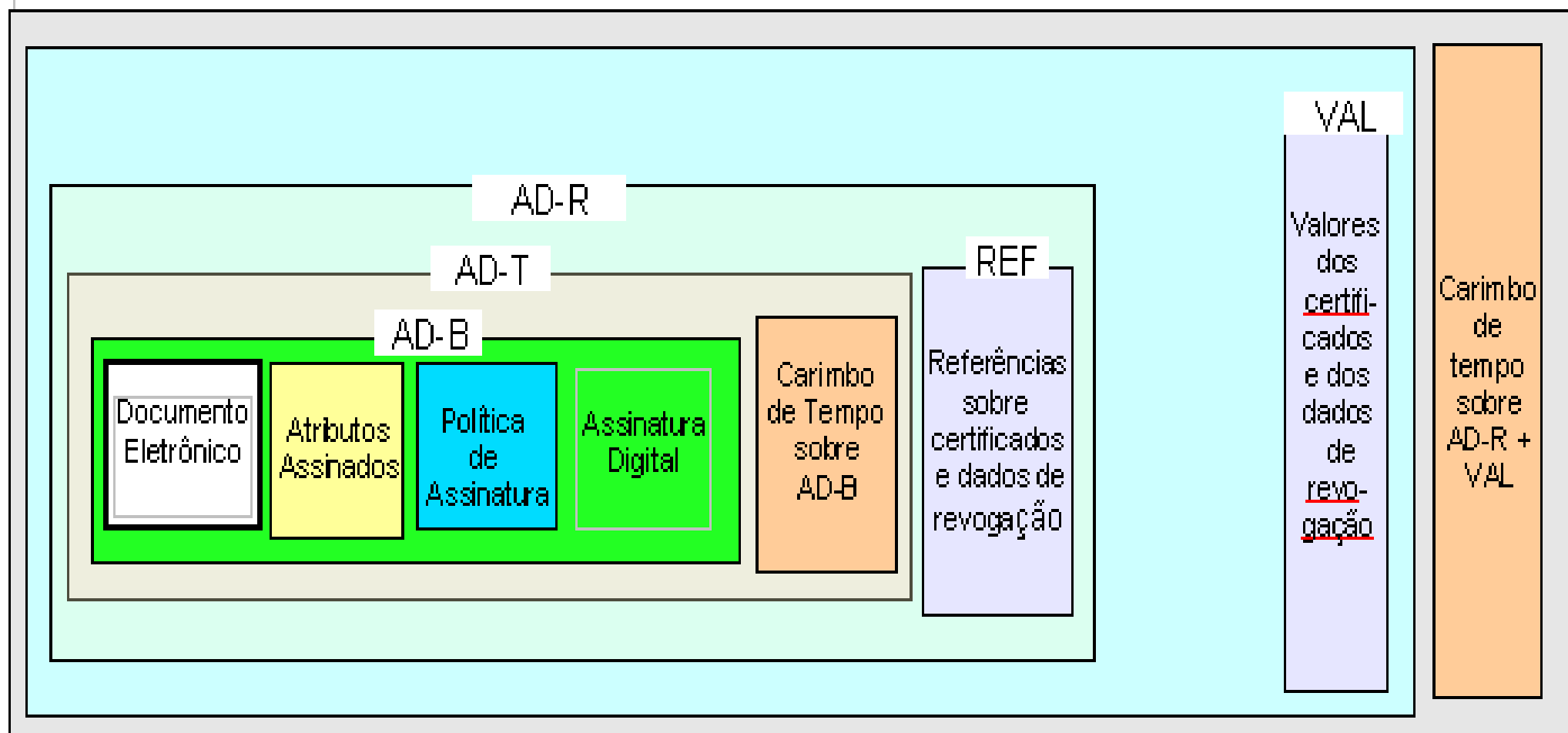


Figura 5e – Assinatura digital com informações para arquivamento (AD-A)

Grato pela atenção

Wilson R. Hirata

Coordenador-Geral de Normalização e Pesquisa
Diretoria de Auditoria, Fiscalização e Normalização
Instituto Nacional de Tecnologia da Informação

wilson.hirata@iti.gov.br

Telefone: 61 3424-3868

www.iti.gov.br