INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

Verificador de Conformidade

Padrão Brasileiro de Assinatura Digital (PBAD)

Ruy Ramos

13º CERTFORUM
FÓRUM DE CERTIFICAÇÃO DIGITAL

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

Agenda

- Padrão Brasileiro de Assinatura Digital (PBAD)
- Verificador de Conformidade
- Principais dúvidas

Padrão de Assinatura Digital

Padrão Brasileiro de Assinatura Digital

Padrão Brasileiro de Assinatura Digital

DOC-ICP-15 Visão Geral sobre Assinaturas Digitais na ICP-Brasil - v.2.1

DOC-ICP-15.01 Requisitos 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.2.1

http://www.iti.gov.br/twiki/bin/view/Certificacao/DocIcp

Referências aos padrões e normas internacionais

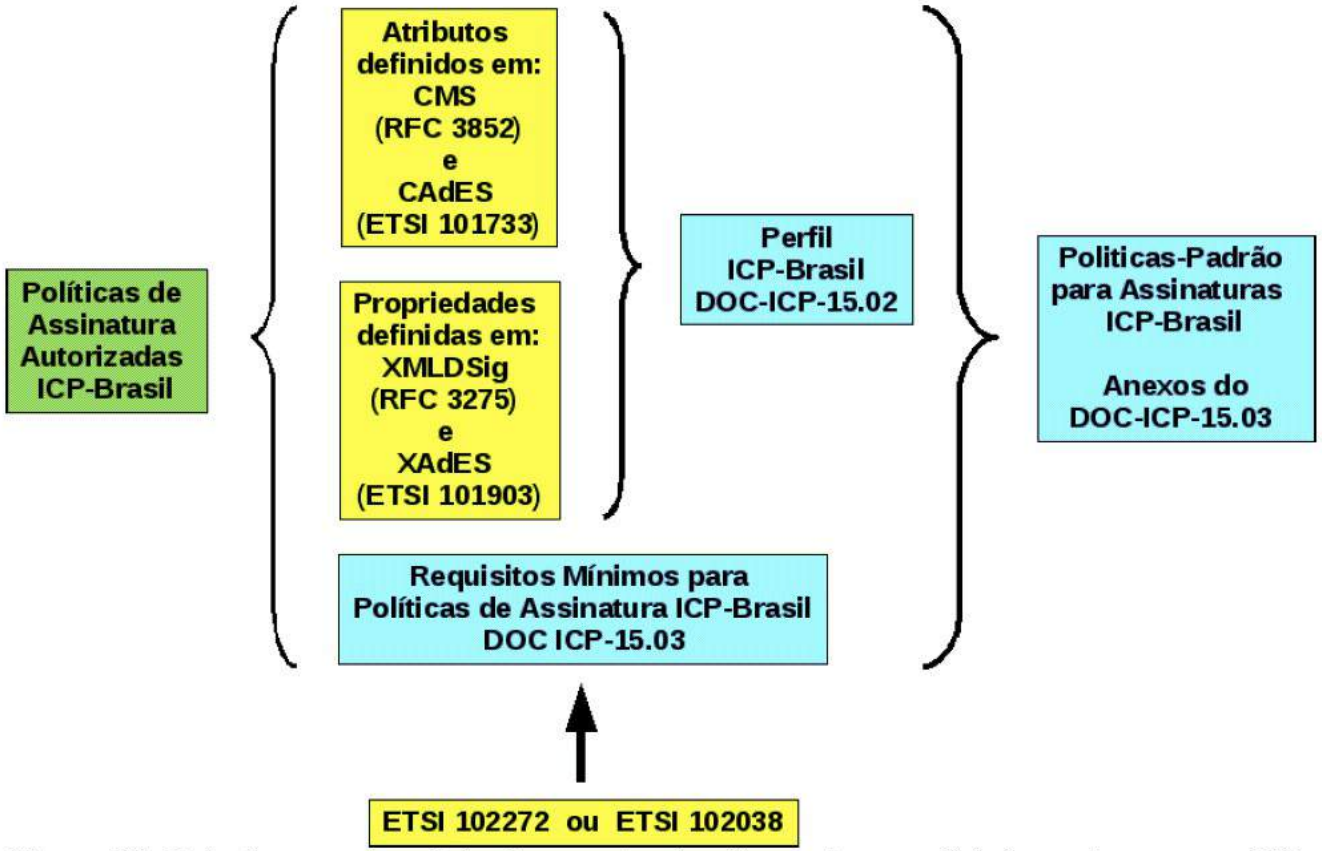


Figura 6.3: Relação entre os padrões internacionais sobre assinatura digital e os documentos ICP-Brasil

~~Futuras~~ referências ao PADES

PAdES Standard (ETSI TS 102 778)

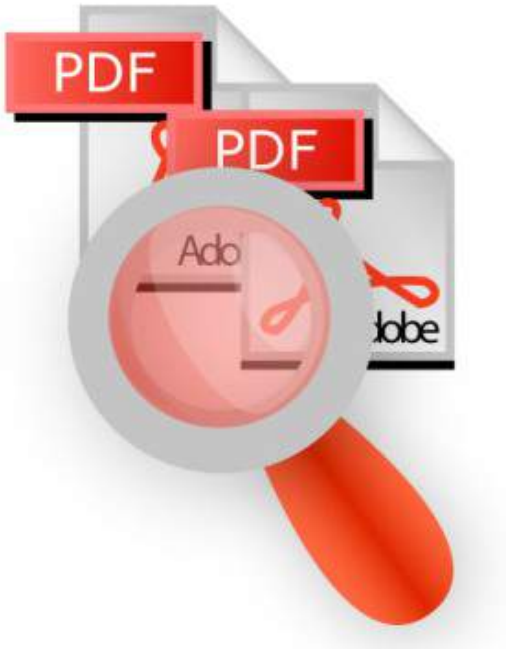
Part 1: PAdES Overview – a framework document for PAdES

Part 2: PAdES Basic – Profile based on ISO 32000-1

Part 3: PAdES Enhanced – PAdES-Basic Electronic Signatures and PAdES-Explicit Policy Electronic Signatures Profiles

Part 4: PAdES Long Term – PAdES-Long Term Validation Profile

Part 5: PAdES for XML Content – Profiles for XAdES signatures of XML content in PDF files

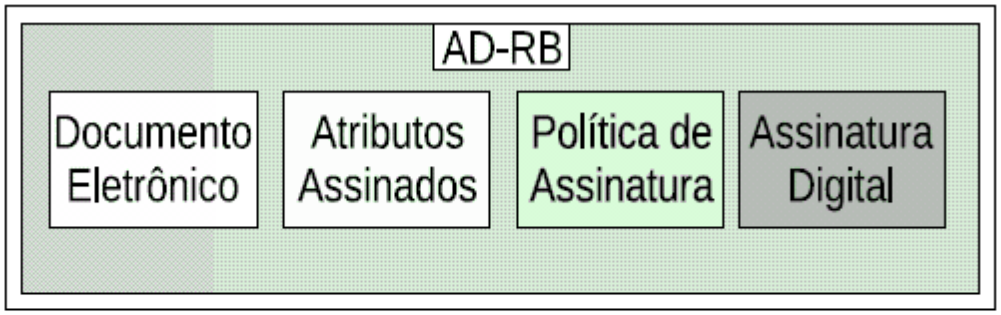


ISO 32000-1:2008

Políticas de Assinatura Digital

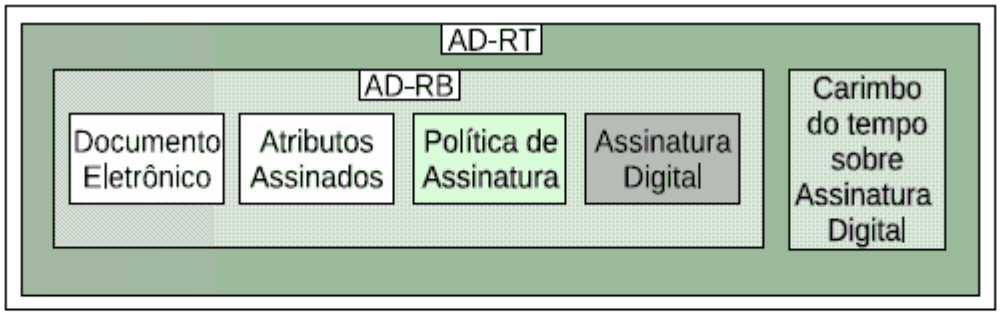
- garantia aos documentos eletrônicos assinados com certificado ICP-Brasil
- preservação de informações e referências (evidências) para futuras consultas ou esclarecer eventuais conflitos (via perícia)
- Interoperabilidade
- Intercâmbio de documentos eletrônicos
- Conformidade às leis e/ou regulamentos

AD de referência básica
AD-RB



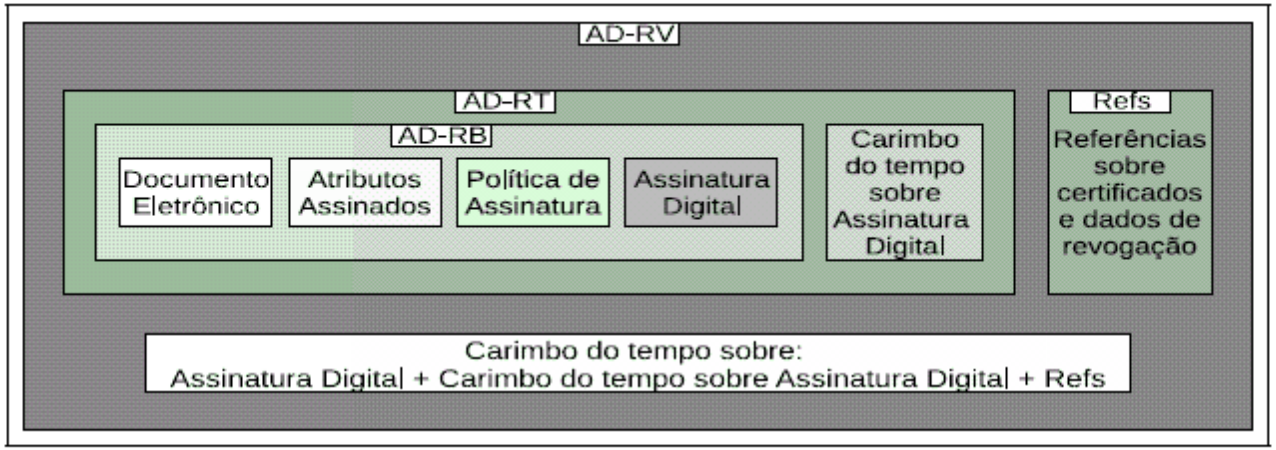
- **Campo de Aplicação**
  - segurança na autenticação do signatário
  - integridade do conteúdo digital
  - sem referências temporais
  - múltiplas assinaturas

AD com referência de tempo
AD-RT



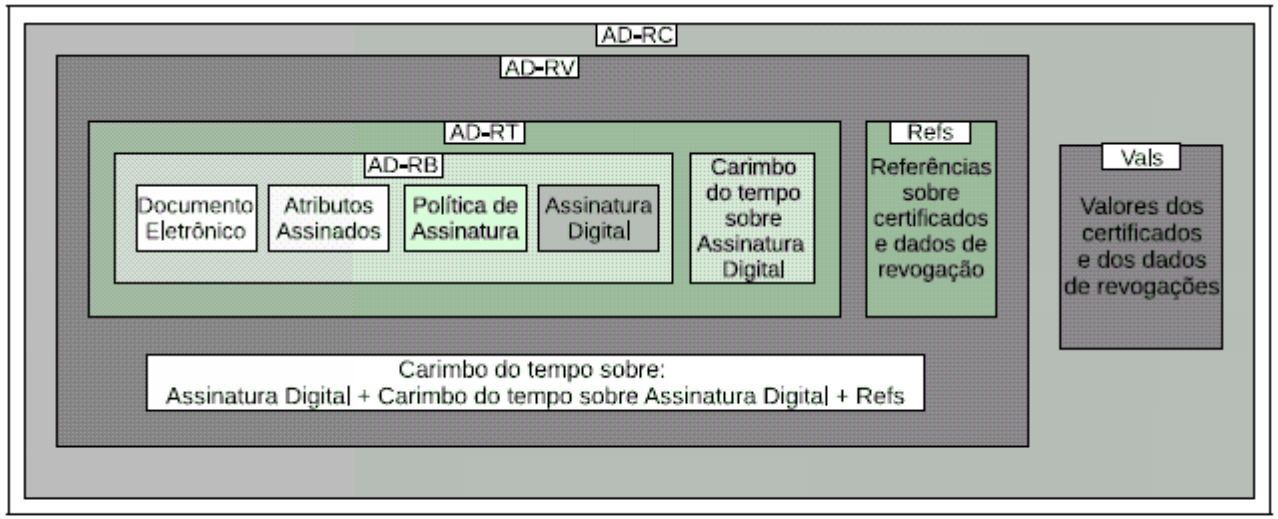
- **Campo de Aplicação**
  - além das propriedades da AD-RB, maior segurança em relação à irretratabilidade do momento de geração
  - referência de tempo
  - LCRs ou respostas OCSP (referências de revogação) obtidos externamente.

AD com referência de validação AD-RV



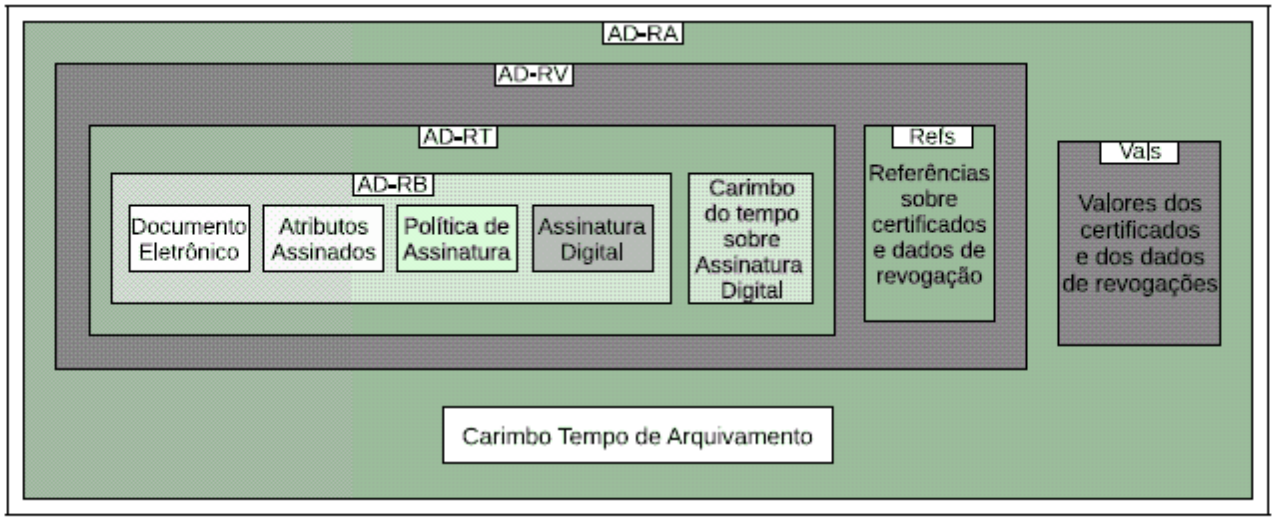
- **Campo de Aplicação**
  - inclui referências sobre a cadeia de certificação
  - referências de revogação (LCR ou resposta OCSP)
  - proteção de mais um carimbo do tempo

AD com referência completa AD-RC



- **Campo de Aplicação**
  - além das referências, guarda os valores da LCR ou resposta OCSP
  - requer maior capacidade de armazenamento
  - possibilita a validação mesmo em situação de contingência da AC

AD com referência para arquivamento AD-RA



- **Campo de Aplicação**
  - além de todas as propriedades anteriores, segurança arquivamento por longos períodos
  - inclusão de novos carimbos do tempo
  - manutenção da segurança criptográfica

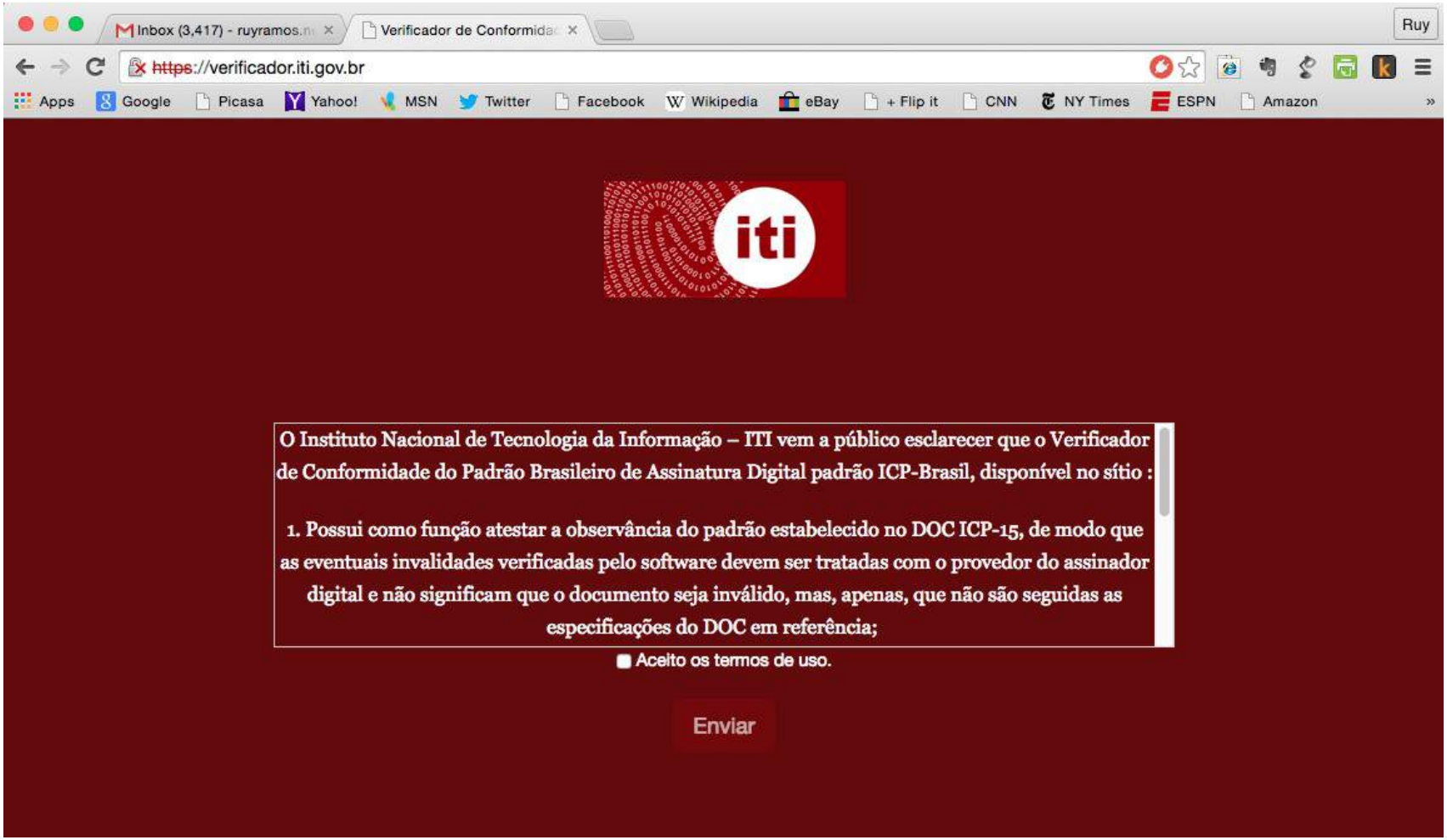
INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

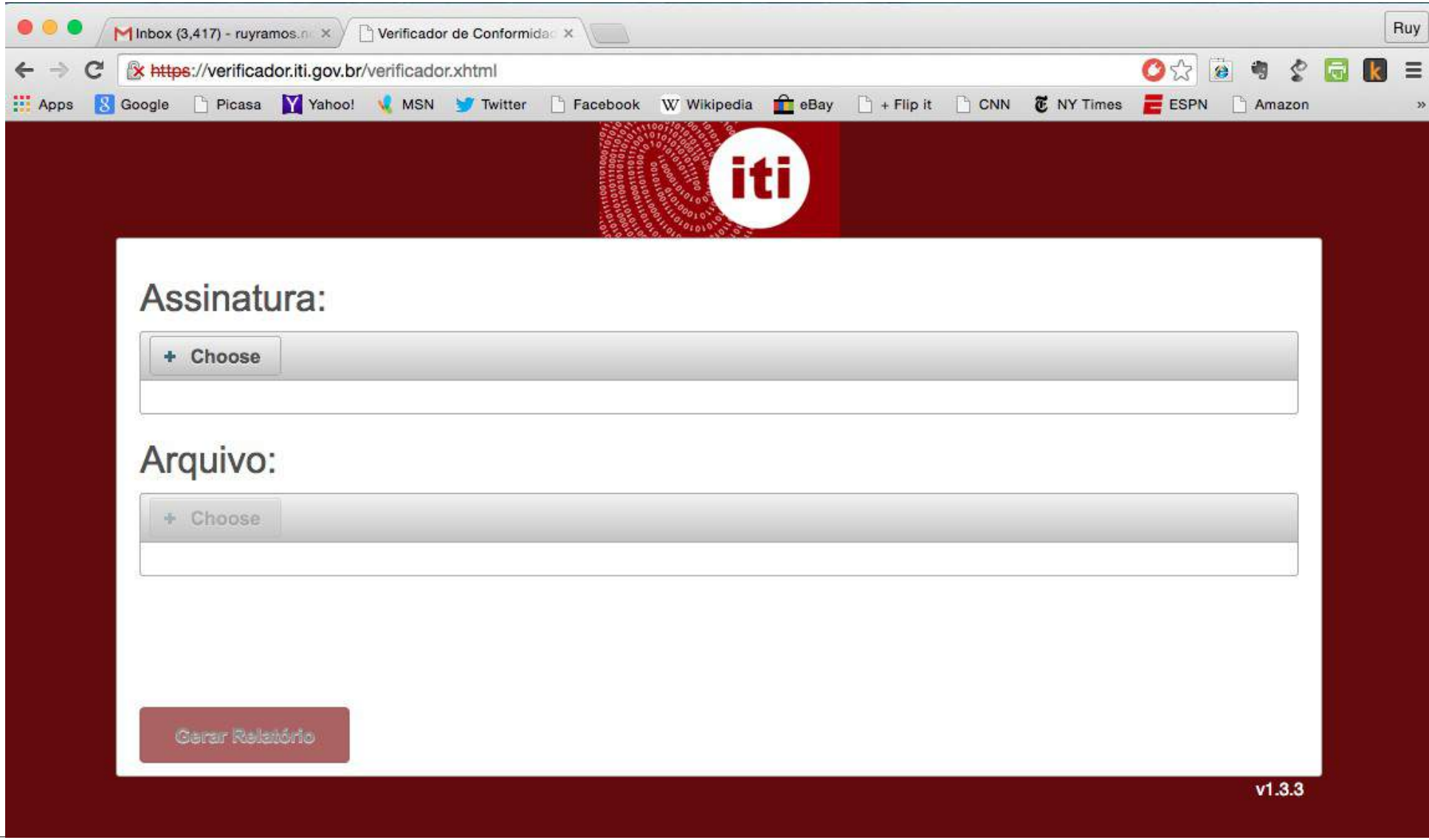
Verificador de Conformidade

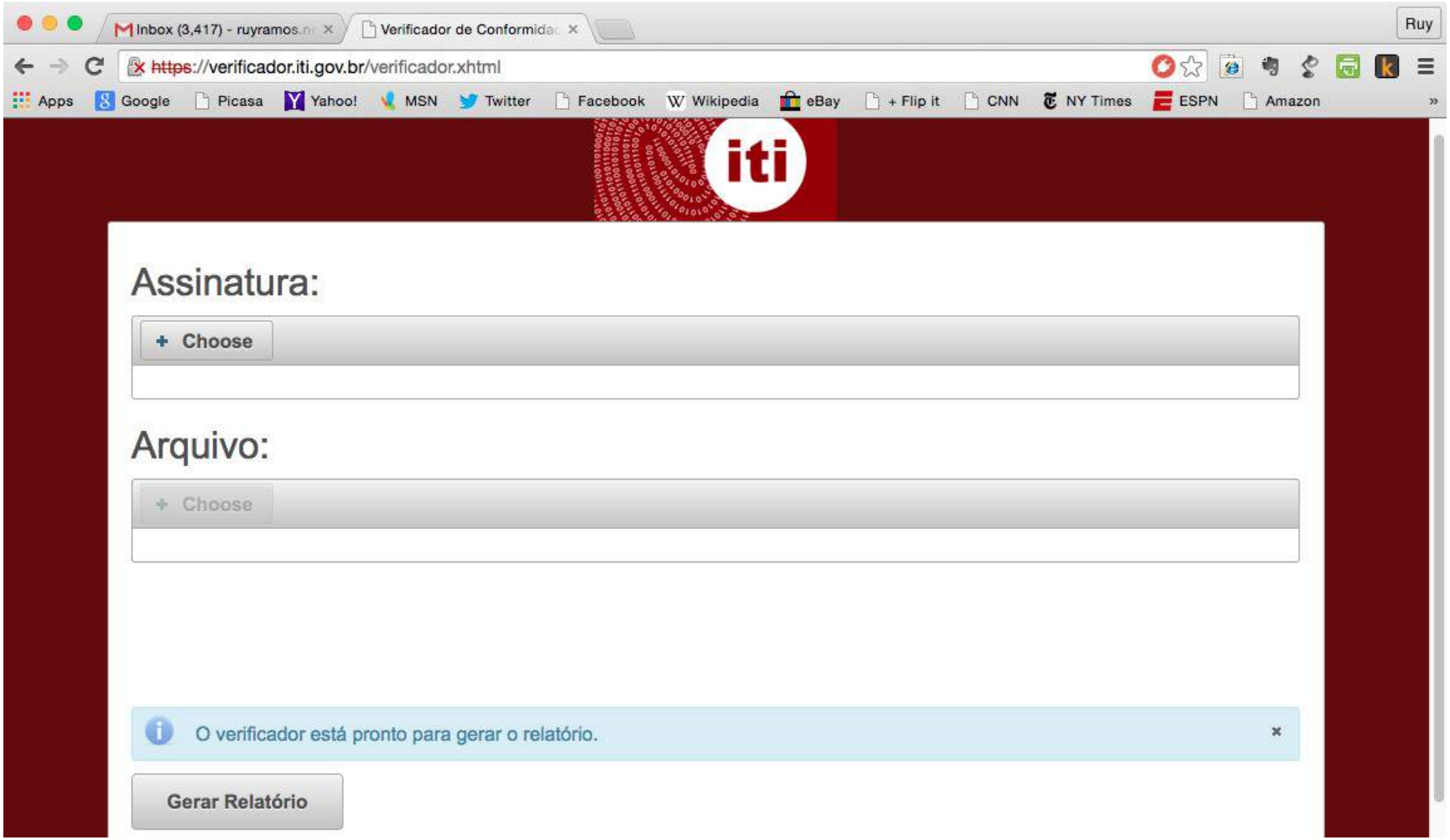
- Validar a conformidade ao PBAD (DOC-ICP-15)

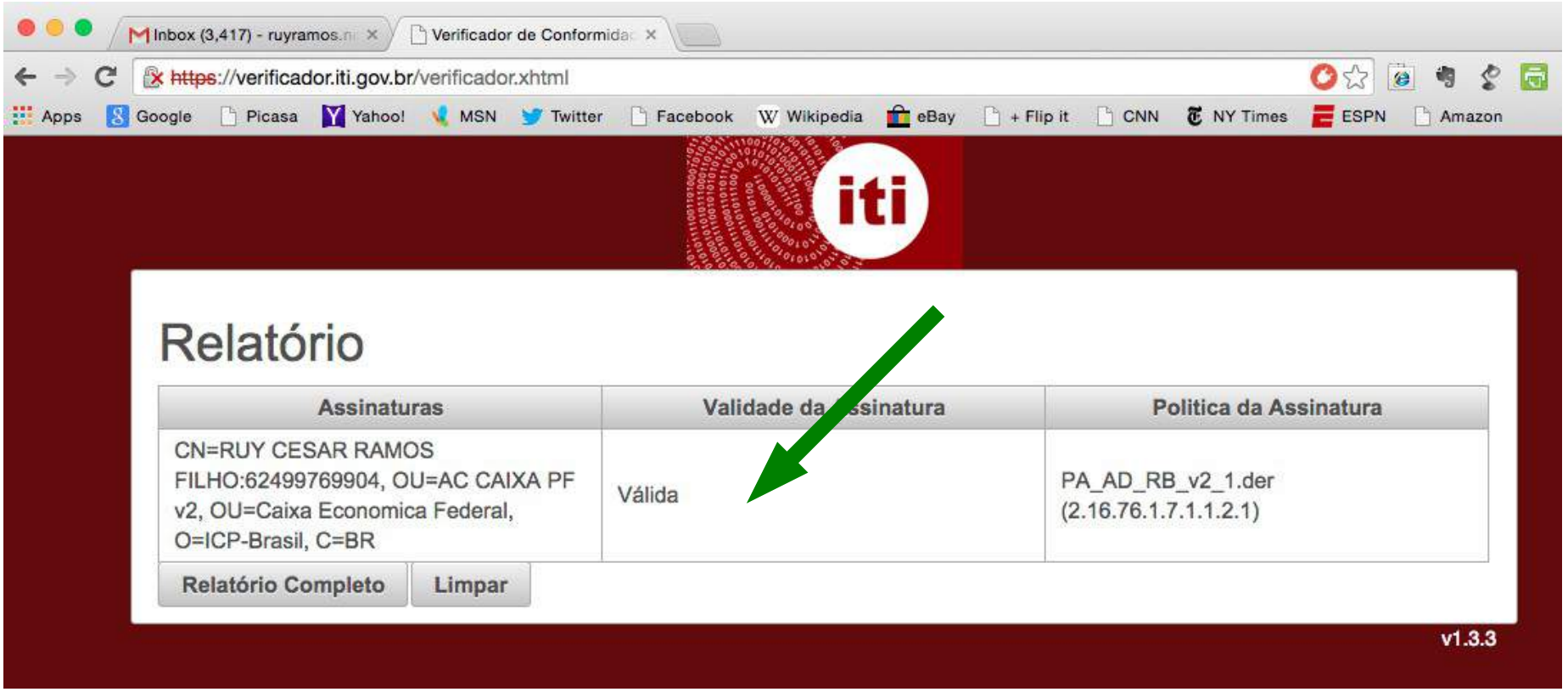
- *Não* confere *autenticidade* ou *validade* ao documento assinado

verificador ≠ *debug*

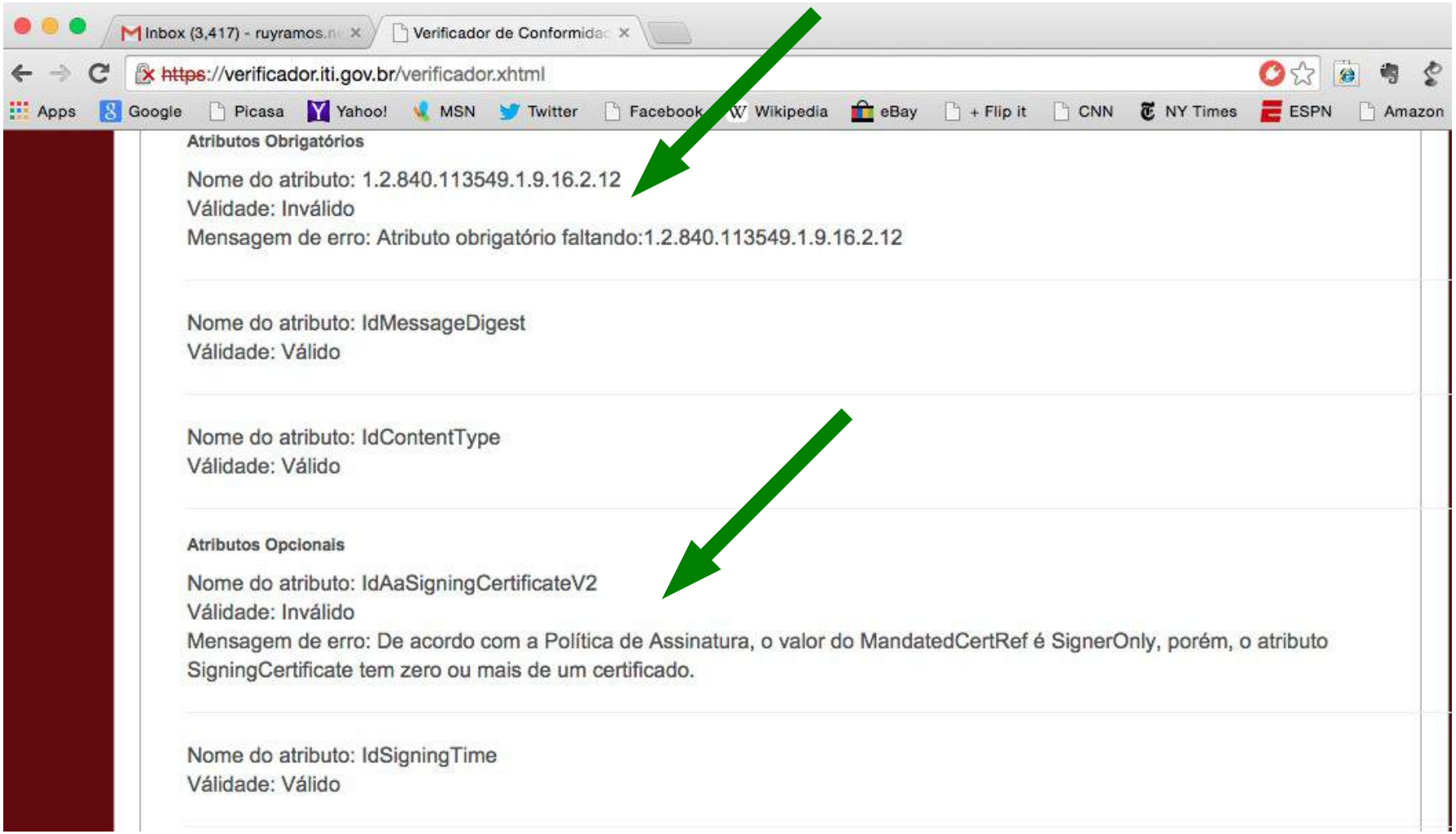

Inbox (3,417) - ruyramos.
Verificador de Conformidad
Ruy
https://verificador.iti.gov.br
Apps
Google
Picasa
Yahoo!
MSN
Twitter
Facebook
Wikipedia
eBay
+ Flip it
CNN
NY Times
ESPN
Amazon
iti
O Instituto Nacional de Tecnologia da Informação – ITI vem a público esclarecer que o Verificador de Conformidade do Padrão Brasileiro de Assinatura Digital padrão ICP-Brasil, disponível no sítio :
1. Possui como função atestar a observância do padrão estabelecido no DOC ICP-15, de modo que as eventuais invalidades verificadas pelo software devem ser tratadas com o provedor do assinador digital e não significam que o documento seja inválido, mas, apenas, que não são seguidas as especificações do DOC em referência;
Aceito os termos de uso.
Enviar


Inbox (3,417) - ruyramos.n
Verificador de Conformidad
Ruy
https://verificador.iti.gov.br/verificador.xhtml
Apps
Google
Picasa
Yahoo!
MSN
Twitter
Facebook
Wikipedia
eBay
+ Flip it
CNN
NY Times
ESPN
Amazon
Assinatura:
+ Choose
Arquivo:
+ Choose
Gerar Relatório
v1.3.3


Inbox (3,417) - ruyramos.
Verificador de Conformida
Ruy
https://verificador.iti.gov.br/verificador.xhtml
Apps
Google
Picasa
Yahoo!
MSN
Twitter
Facebook
Wikipedia
eBay
+ Flip it
CNN
NY Times
ESPN
Amazon
Assinatura:
+ Choose
Arquivo:
+ Choose
O verificador está pronto para gerar o relatório.
Gerar Relatório


Inbox (3,417) - ruyramos.
Verificador de Conformida
https://verificador.iti.gov.br/verificador.xhtml
Apps
Google
Picasa
Yahoo!
MSN
Twitter
Facebook
Wikipedia
eBay
+ Flip it
CNN
NY Times
ESPN
Amazon
Relatório
Assinaturas
Validade da Assinatura
Politica da Assinatura
CN=RUY CESAR RAMOS FILHO:62499769904, OU=AC CAIXA PF v2, OU=Caixa Economica Federal, O=ICP-Brasil, C=BR
Válida
PA_AD_RB_v2_1.der (2.16.76.1.7.1.1.2.1)
Relatório Completo
Limpar
v1.3.3


Relatório
Assinaturas
Validade da Assinatura
Politica da Assinatura
CN=RUY CESAR RAMOS FILHO:62499769904, OU=AC CAIXA PF v2, OU=Caixa Economica Federal, O=ICP-Brasil, C=BR
Inválida
PA_AD_RT_v2_1.der (2.16.76.1.7.1.2.2.1)
Relatório Completo
Limpar
v1.3.3


Inbox (3,417) - ruyramos.n
Verificador de Conformidac
https://verificador.iti.gov.br/verificador.xhtml
Apps
Google
Picasa
Yahoo!
MSN
Twitter
Facebook
Wikipedia
eBay
+ Flip it
CNN
NY Times
ESPN
Amazon
Atributos Obrigatórios
Nome do atributo: 1.2.840.113549.1.9.16.2.12
Válidade: Inválido
Mensagem de erro: Atributo obrigatório faltando:1.2.840.113549.1.9.16.2.12
Nome do atributo: IdMessageDigest
Válidade: Válido
Nome do atributo: IdContentType
Válidade: Válido
Atributos Opcionais
Nome do atributo: IdAaSigningCertificateV2
Válidade: Inválido
Mensagem de erro: De acordo com a Política de Assinatura, o valor do MandatedCertRef é SignerOnly, porém, o atributo SigningCertificate tem zero ou mais de um certificado.
Nome do atributo: IdSigningTime
Válidade: Válido

FAQ

- "*Montei um artefato na política RB e coloquei um carimbo e o verificador dá erro*?!"
- " … a nota fiscal eletrônica dá erro, o verificador não dá nenhuma mensagem!"
- " … estou usando uma RT com um carimbo de teste e o verificador não reconhece!"
- "recebi este arquivo assinado em PDF … o verificador nem analisa ..."

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

Orientações

- Certifique-se que o assinador produz no padrão DOC-ICP-15 (consulte seu fornecedor)
- Submeta o arquivo assinado e analise o relatório e em caso de dúvida procure seu provedor de solução
- O verificador de conformidade é aperfeiçoado e corrigido (quando alguma falha é encontrada)
- Envie sugestões para *verificador@iti.gov.br*

Perguntas ?

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO

Ruy Ramos

ruy.ramos@iti.gov.br

www.iti.gov.br

ICP Brasil

O Brasil na era da certificação digital