

	ORGANIZAÇÃO DA DOCUMENTAÇÃO PARA O PROCESSO DE AVALIAÇÃO DE SOFTWARE	NORMA N.º NIT-SINST-003	REV. N.º 01
		PUBLICADO EM OUT/2018	PÁGINA 1/26

SUMÁRIO

- 1 Objetivo**
- 2 Campo de aplicação**
- 3 Responsabilidade**
- 4 Documentos de referência**
- 5 Documentos complementares**
- 6 Definições**
- 7 Entrega da documentação**
- 8 Conteúdo do pacote de entrega**
- 9 Padrão de estrutura de diretórios**
- 10 Requisitos de assinatura digital**
- 11 Relatório de ensaio de laboratório externo**
- 12 Histórico da revisão e quadro de aprovação**
- ANEXO A – Chave pública do Sinst**
- ANEXO B – Modelo de declaração de vínculo**
- ANEXO C – Chaves para teste de assinatura digital**
- ANEXO D – Exemplos de assinaturas digitais para chaves criptográficas de teste**
- ANEXO E - Exemplo de procedimento, resultado e conclusão para relatório de ensaio**

1 OBJETIVO

Estabelecer os requisitos de organização e apresentação da documentação de software e hardware para os instrumentos que possuem requisitos técnicos de segurança de software e hardware em seus respectivos RTM.

2 CAMPO DE APLICAÇÃO

Essa norma se aplica ao Dimel/Disme/Sinst, aos laboratórios acreditados em ensaios de software no âmbito da metrologia legal e aos requerentes que submetem instrumentos de medição ao processo de avaliação de software.


3 RESPONSABILIDADE

A responsabilidade pela aprovação, revisão e cancelamento desta Norma é do Sinst.

4 DOCUMENTOS DE REFERÊNCIA

NIT-Sinst-020	Requisitos do protocolo de comunicação serial para verificação de integridade de software em instrumentos de medição
FIPS 186-4	<i>Digital Signature Standard</i>
FIPS 180-4	<i>Secure Hash Standard</i>

(Continua)

	NIT-SINST-003	REV. 01	PÁGINA 2/32
---	----------------------	--------------------	------------------------

FIPS 198-1	<i>The Keyed-Hash Message Authentication Code (HMAC)</i>
Portaria nº 150, de 29 de março de 2016.	Vocabulário Internacional de Termos de Metrologia Legal
ISO 32000	<i>Document management -- Portable document format</i>
Stallings, W. (2013)	<i>Cryptography and Network Security: Principles and practice, prentice Hall Press, Upper Saddle River, NJ, USA</i>

5 DOCUMENTOS COMPLEMENTARES

FOR-Dimel-023	Solicitação de assinatura digital de arquivos/programas
FOR-Dimel-024	Descrição simplificada da arquitetura de hardware e software
FOR-Dimel-060	Termo de confidencialidade e imparcialidade da Dimel

6 DEFINIÇÕES

6.1 Siglas

As siglas das UP/UO do Inmetro podem ser acessadas em <http://intranet.inmetro.gov.br/tema/qualidade/docs/pdf/siglas-inmetro.pdf>.


CRC	<i>Cyclic Redundancy Code</i>
DVIS	Dispositivo de verificação de integridade de software
<i>OpenPGP</i>	Padrão aberto de criptografia conforme a RFC4880
pdf	<i>Portable document format</i>
RTM	Regulamento Técnico Metrológico
UML	<i>Unified Modeling Language</i>
UTF-8	<i>8-bit Unicode transformation format</i>
DSA	<i>Digital Signature Algorithm</i>
ECDSA	<i>Elliptic Curve Digital Signature Algorithm</i>
RSA	<i>Sistema de criptografia de chave pública Rivest-Shamir-Adleman</i>
PSS	<i>Probabilistic Signature Scheme</i>
SHA-256	<i>Secure Hash Algorithm 2 com valor de hash de 256 bits</i>

6.2 Termos

6.2.1 Análise da documentação de software – Exame da documentação textual que comprova o atendimento aos requisitos técnicos de segurança de software e hardware do RTM do respectivo instrumento.

6.2.2 Análise de código fonte – Exame do código fonte do software embarcado no instrumento com intuito de verificar o atendimento aos requisitos técnicos de segurança de software e hardware do RTM do respectivo instrumento.

6.2.3 Arquivo .hex – Formato de arquivo que transmite informação binária no formato de texto ASCII.

 INMETRO	NIT-SINST-003	REV. 01	PÁGINA 3/32
---	----------------------	--------------------	------------------------

6.2.4 Assinatura digital - Código atribuído a um arquivo digital de forma a provar a sua integridade, autenticidade e não repúdio.

6.2.5 Carga de software - Processo de transferência automática de software para o instrumento de medição usando qualquer meio apropriado local ou remoto sem a necessidade de romper selagem principal.

6.2.6 Chave privada - No contexto de assinaturas digitais, é a chave criptográfica utilizada para assinar um arquivo. Pertence a quem assinou o arquivo e não deve ser divulgada. No contexto de confidencialidade a chave privada é a chave criptográfica utilizada para decifrar a mensagem criptografada com a chave pública.

6.2.7 Chave pública - No contexto de assinaturas digitais, é a chave criptográfica utilizada para verificar assinaturas digitais gerada pela chave privada relacionada. No contexto de confidencialidade a chave pública é a chave criptográfica utilizada para cifrar a mensagem permitindo que apenas o detentor da chave privada tenha acesso ao conteúdo da mensagem. É computacionalmente inviável encontrar a chave privada a partir da chave pública, o que permite ampla divulgação dessa chave.

6.2.8 Computacionalmente inviável – Uma computação que requer uma quantidade de recursos muito maior que os disponíveis com a tecnologia atual. De outra forma, um problema de criptografia é dito computacionalmente inviável se uma máquina de Turing probabilística tem probabilidade negligível de resolver o problema.

6.2.9 Compilação assistida - Quando a compilação dos binários legalmente relevantes é feita na presença do técnico do Inmetro ou do laboratório acreditado.

6.2.10 Declaração de vínculo (entre o código fonte entregue ao Inmetro e os programas executáveis gerados) - Documento que afirma o vínculo entre o código fonte e o software embarcado no instrumento.

6.2.11 Descrição funcional - Documento textual que descreve a arquitetura e os conceitos de projeto do instrumento, bem como as principais tecnologias utilizadas na sua fabricação. Os principais elementos de hardware e de software que compõe a cadeia metrológica legalmente relevante devem ser claramente descritos, bem como a lista completa de funcionalidades oferecidas pelo instrumento.


6.2.12 Documentação - Documentos contidos no pacote de entrega. Sinônimo de documentação de software.

6.2.13 Ensaio funcional – Testes para verificar o atendimento aos requisitos técnicos de segurança de software e hardware do RTM do instrumento quando diversas entradas são aplicadas no instrumento observando-se também as componentes físicas do instrumento.

6.2.14 Ensaio de Software – Procedimento técnico que visa a análise dos requisitos técnicos de software e hardware por meio de análise da documentação de software, análise do código fonte (quando pertinente) e ensaio funcional.

6.2.15 Esquemático eletrônico - Desenho técnico que apresenta através de símbolos padronizados a conexão dos componentes de um circuito eletrônico.

6.2.16 Estado - Estabelece o atual conjunto de condições do sistema. Em um determinado estado o sistema apresenta um comportamento, aguarda por um gatilho ou executa alguma ação.

	NIT-SINST-003	REV. 01	PÁGINA 4/32
---	----------------------	--------------------	------------------------

6.2.17 Gestor do processo do Sinst - Responsável por coordenar administrativamente os processos de avaliação de software no Sinst.

6.2.18 *Hash* criptográfico - Função matemática, que mapeia valores de um bloco de dados, em um número de tamanho fixo e reduzido (código *hash*) com as seguintes propriedades:

- a) A mudança em qualquer bit de um bloco de dados implica em um código hash diferente;
- b) Não é viável a partir de um código hash retornar ao bloco de dados original; e,
- c) Não é viável encontrar dois blocos que gerem o mesmo código hash.

6.2.19 *Hash* de identificação do pacote de entrega – O pacote de entrega a ser depositado no processo de avaliação de software consiste em único arquivo compactado (tar, zip, etc.). O *hash* SHA-256 desse arquivo compactado, sem estar criptografado, é o *hash* de identificação do pacote de entrega.

6.2.20 *Hash* final da documentação - *Hash* SHA-256 do arquivo do pacote de entrega criptografado com a chave pública do Sinst para uma documentação aprovada no processo de avaliação de software.

6.2.21 Imagem vetorizada - Imagem com codificação baseada em polígonos.

6.2.22 Manual operacional - Documento textual que explicita a operação do equipamento e seu software.

6.2.23 Manual de instalação - Documento textual que explicita a instalação do instrumento de medição.

6.2.24 Modelo – Modelo definitivo de um instrumento de medição no qual todos os elementos que afetam suas propriedades metrológicas são adequadamente definidos.

6.2.25 Módulo – Parte do software legalmente relevante capaz de executar uma funcionalidade bem definida de forma independente.

6.2.26 Pacote de entrega - Conjunto de arquivos digitais a ser entregue a Dimel/Disme/Sinst, para serem analisados em um processo de avaliação de software.


6.2.27 Processo de avaliação de software – Processo realizado pela diretoria de metrologia legal que visa a análise dos requisitos técnicos de segurança de software e hardware referentes ao RTM do instrumento em análise.

6.2.28 Verificação de integridade - Processo que verifica que os dados/software/parâmetros não foram alterados durante o uso, reparo, manutenção, transferência ou armazenamento sem que haja a autorização.

7 ENTREGA DA DOCUMENTAÇÃO

7.1 Entrega da documentação à Dimel

7.1.1 A documentação deverá ser entregue ao gestor do processo presencialmente ou online durante o processo de avaliação de software. O atraso na entrega da documentação pode levar ao cancelamento do processo.

	NIT-SINST-003	REV. 01	PÁGINA 5/32
---	----------------------	--------------------	------------------------

7.1.2 Na entrega presencial, o pacote de entrega deve estar gravado em mídia física do tipo "Apenas leitura" (ex.: CD-R, DVD-R)

7.1.3 Na entrega online o pacote de entrega deve ser disponibilizado em servidor online. Nesse caso, deve ser enviado ao gestor do processo, por e-mail, as instruções para descarga do arquivo.

Nota - A política de rede do Inmetro pode impedir o uso de algumas ferramentas para transferência de arquivos. O requerente deve entrar em contato com o gestor do processo para acordar as ferramentas que serão utilizadas para a transferência de arquivo e que estejam disponíveis para ambos.

7.1.4 A documentação textual deve ser entregue em língua portuguesa. Será aceito comentários em código fonte feitos na língua portuguesa ou inglesa. Manuais técnicos de componentes do sistema (por exemplo, *datasheet* de microcontroladores, documentação de bibliotecas, etc.) podem ser entregue em língua inglesa.

7.2 Entrega da documentação à Dimci ou ao laboratório acreditado

7.2.1 No caso da entrega de documentação à Dimci ou ao laboratório acreditado deve se observar os mesmos requisitos de organização e segurança dessa norma, salvo que a chave pública utilizada para criptografar o pacote de entrega deve ser fornecida pela Dimci ou pelo laboratório acreditado.

7.3 Confidencialidade e segurança da informação

7.3.1 O pacote de entrega é composto de um único arquivo cifrado, em formato *OpenPGP*.

7.3.2 Todos os documentos descritos no item 8 devem ser compactados (zip, tar, rar, etc) em um único pacote.

7.3.2.1 Deve-se calcular o *hash* SHA-256 do pacote compactado. Esse é o *hash* de identificação do pacote de entrega.

7.3.3 O pacote compactado deve ser criptografado em formato *OpenPGP*. Para efetuar a encriptação, deve ser utilizada a chave pública da Dimel/Dime/Sinst, conforme explicado no anexo A.


7.3.3.1 Não se devem incluir múltiplos arquivos compactados ou agrupados em pacotes ou ainda com necessidade de senha para abertura. Toda segurança é garantida pela encriptação do arquivo compactado em formato *OpenPGP*.

7.3.3.2 Não deve-se incluir arquivos encriptados dentro do pacote já encriptado, bastando uma única camada de criptografia. Toda segurança é garantida pela encriptação do arquivo compactado em formato *OpenPGP*.

7.3.4 Ao entregar o arquivo o requerente deve enviar também o *hash* SHA-256 de identificação do pacote de entrega, conforme calculado 7.3.2.1.

7.4 Formulários

7.4.1 Junto ao pacote de entrega, devidamente criptografado, o requerente deve enviar o FOR-Dimel-024 devidamente preenchido.

	NIT-SINST-003	REV. 01	PÁGINA 6/32
---	----------------------	--------------------	------------------------

7.4.2 Caso o instrumento realize carga de software, o requerente deve enviar o formulário FOR-Dimel-023, devidamente preenchido.

7.5 Nomeação do arquivo

7.5.1 O arquivo deve ser nomeado da seguinte forma:

[requerente]_[número do processo]_[modelo]_[versão da documentação][revisão da documentação][aaaammdd].zip.gpg

Em que:

- a) requerente (Campo textual): Deve conter o nome do requerente.
- b) número do processo (Campo numérico): Deve conter o número do processo Orquestra.
- c) modelo (Campo textual): Deve conter o nome do modelo ao qual a documentação está associada.
- d) versão da documentação (Campo numérico): Para controle da versão da documentação submetida ao Sinst. Deve conter um número de versão, iniciando em 001, que deve ser acrescido de uma unidade sempre o que o software passar por um novo processo de avaliação de software.
- e) Revisão da documentação: Campo numérico iniciando em 001. É comum no processo de avaliação de software que o requerente faça modificações no pacote de entrega no intuito de corrigir não conformidades identificadas. Toda vez que o pacote for reenviado ao Sinst o número associado à revisão da documentação deve ser acrescido em uma unidade.
- f) aaaammdd: É data de quando a documentação foi enviada ao Sinst no formato ano, com quatro dígitos, seguido de mês, com dois dígitos, seguido de dia, com dois dígitos.

Nota - a versão da documentação descrita na alínea “d” não têm relação com o identificador único informado pelo requerente nem com a versão dos softwares submetidos no processo.

7.6 Formatação dos arquivos textuais

7.6.1 Dois tipos de formatos de arquivos são aceitos para os documentos textuais que compõe o pacote de entrega: formatos de arquivos em texto pleno e em pdf.

7.6.2 A codificação para arquivos em texto pleno deve ser no formato UTF-8.


7.6.3 O memorial descritivo e documentação anexa devem ser enviados em pdf enquanto código fonte deve ser enviado em texto pleno.

7.6.4 O nome dos arquivos contidos no pacote de entrega deve evidenciar o conteúdo dos mesmos, preferencialmente utilizando o título do documento ou um mnemônico que o represente.

Nota 1 - O pacote de entrega pode conter outros tipos de arquivos, como software, arquivos .hex, fotos, etc.

Nota 2 - Não enviar árvore de diretório com mais de 256 caracteres em função de limitações do uso do win XP.

7.6.5 Todo documento, que não seja de terceiros, (*datasheet*, etc), deve informar a versão do software legalmente relevante o qual ele documenta.

	NIT-SINST-003	REV. 01	PÁGINA 7/32
---	----------------------	--------------------	------------------------

7.7 Desenhos

7.7.1 Quaisquer desenhos devem caracterizar claramente o instrumento de medição ou parte desenhada. Eles devem ser fornecidos no MOD-Dimel-037, em meio eletrônico no formato pdf.

7.7.2 O pdf deve ser construído a partir de uma imagem vetorizada que permita ampliação.

7.8 Atualização de documento

7.8.1 Dentro de um mesmo processo de avaliação de software, cada documento deve manter o mesmo nome de arquivo da versão anterior de forma a facilitar a comparação de alteração entre diretórios.

7.8.2 Cada documento deve ter um controle de revisão, explicitando as alterações sofridas.

8 CONTEÚDO DO PACOTE DE ENTREGA

8.1 Documentação geral

8.1.1 Descrição funcional

8.1.1.1 A descrição funcional deve conter:

- a) descrição das partes envolvidas na medição, cálculo e processamento do valor de medição;
- b) partes envolvidas no armazenamento (persistência), transmissão e exibição dos dados de medição;
- c) partes envolvidas na configuração do sistema;
- d) partes envolvidas na geração de alarmes (sensores); e,
- e) partes envolvidas na proteção dos elementos que compõem o sistema de medição.

8.1.1.2 Alguns itens devem ser detalhados em sessões separadas. Caso um sistema operacional seja requerido, descrever a versão e as atualizações do sistema operacional (como no caso de *service pack* do Windows ou nome e versão da distribuição Linux).

8.1.2 Manual operacional

8.1.2.1 Devem ser descritos todos os modos de configuração possíveis para o instrumento e os respectivos modos de operação para cada configuração.


Nota - Caso seja de interesse, o requerente pode dividir esse documento em mais de um arquivo.

8.1.3 Manual de instalação

8.1.3.1 Devem ser descritos os respectivos modos de instalação do instrumento.

Nota 1 - Caso seja de interesse, o requerente pode dividir esse documento em mais de um arquivo.

Nota 2 - O requerente pode concatenar o manual de instalação com o manual operacional.

	NIT-SINST-003	REV. 01	PÁGINA 8/32
---	---------------	------------	----------------

8.1.4 Declaração de vínculo

8.1.4.1 Caso o RTM requeira a entrega de arquivos de código fonte, no âmbito de um processo de avaliação de software no Inmetro o requerente deve incluir, na documentação, a declaração afirmando o vínculo entre o código fonte e o software embarcado no instrumento. Um modelo de declaração de vínculo é apresentado no anexo B.

8.1.5 Descrição técnica de como gerar os programas executáveis entregues ao Inmetro

8.1.5.1 Caso o RTM requeira a entrega de arquivos de código fonte o requerente deve também fornecer um procedimento explicitando como obter os binários legalmente relevantes a partir do código fonte fornecido. Esse procedimento deve ser detalhado, explicitando compilador, assembler, linker, configurações de sistemas, bibliotecas, plataforma, sistema operacional, hardware necessário ou configuração de máquina virtual, etc.

8.1.5.2 Caso o requerente opte por uma arquitetura com uso de assinatura digital, aonde a entrega de código fonte é parcial, o procedimento deve explicitar como obter os binários legalmente relevantes que atuam até o momento da assinatura digital.

8.1.6 Caso o RTM associado ao instrumento não requeira o código fonte, não se faz necessário atender aos requisitos do item 8.1.5.

8.2 Especificações do hardware

8.2.1 Descrição da arquitetura

8.2.1.1 Descrição completa do hardware contemplando a sua arquitetura em módulo, processamento, memórias persistentes, memórias voláteis, interfaces de comunicação etc.

8.2.2 Diagrama de blocos

8.2.2.1 Diagrama de blocos funcionais para cada módulo.

8.2.3 Diagrama esquemático


8.2.3.1 Diagrama esquemático de todas as placas eletrônicas e dispositivos do instrumento. Esses esquemáticos devem ser documentados com o uso de desenhos técnicos conforme descrito no item 7.6.

8.2.4 Leiaute das placas

8.2.4.1 Fotos e/ou desenhos das placas eletrônicas contendo clara visualização do seu leiaute definitivo e a disposição dos componentes nas placas.

8.2.5 Conexões

8.2.5.1 Fotos e/ou desenhos com a descrição das conexões eletrônicas entre placas e dispositivos de hardware do instrumento (cabos de alimentação, controle e comunicação de dados).

	NIT-SINST-003	REV. 01	PÁGINA 9/32
---	---------------	------------	----------------

8.2.6 Interfaces

8.2.6.1 Especificação das interfaces de comunicação do instrumento - devem ser descritas todos os tipos de interface de comunicação presentes no instrumento por meio das suas especificações técnicas e respectivos protocolos de comunicação.

8.3 Especificações do software legalmente relevante

8.3.1 Descrição da arquitetura

8.3.1.1 Descrição da arquitetura do software e suas características de implementação - devem ser descritos os principais blocos do software legalmente relevante, com apresentação de fluxogramas e algoritmos.

8.3.2 Diagrama de blocos

8.3.2.1 Diagrama de blocos/fluxogramas explicitando o fluxo de funcionamento do programa de cada módulo.

8.3.2.2 Diagrama de atividades

8.3.2.2.1 Fluxograma descrevendo a mudança de uma atividade realizada pelo módulo para outra atividade. Deve ser entregue utilizando UML.

8.3.2.3 Diagrama de estados

8.3.2.3.1 Diagrama de transições de estados de cada módulo. Deve ser entregue utilizando UML.

Nota - O diagrama de atividades e de estados são complementares. O diagrama de estado descreve em cada nó o estado em que o sistema se encontra enquanto o diagrama de atividades descreve em cada nó a atividade que causa a transição entre estados.

8.3.2.4 Diagrama de classes

8.3.2.4.1 Caso software legalmente relevante seja programado com orientação a objeto, deve-se fornecer o diagrama de classes. Deve ser entregue utilizando UML.


8.3.3 Descrição funcional das interfaces de usuário

8.3.3.1 Deve incluir a descrição de telas, janelas, menus e diálogos que tenham efeito em dados, parâmetros e no software legalmente relevante.

8.3.4 Lista de comandos e funções ativados por meio das interfaces de usuário e de comunicação

8.3.4.1 Deve descrever os efeitos em funções, dados e parâmetros no software legalmente relevante, e as correspondentes ações passíveis de serem desencadeadas no instrumento.

8.3.5 Código fonte

	NIT-SINST-003	REV. 01	PÁGINA 10/32
---	----------------------	--------------------	-------------------------

8.3.5.1 Caso o RTM do instrumento requeira, o código fonte do software legalmente relevante deve estar contido na documentação em arquivos de texto pleno, codificados UTF-8.

8.3.6 Mapa do vinculador (*linker map file*)

8.3.6.1 Caso o RTM do instrumento requeira entrega de código fonte, deve ser apresentado o mapa de links que mostra como as diferentes sessões de um programa são associadas aos endereços de memória, apresentando o tamanho e o tipo de memória utilizado por cada sessão.

8.4 Memorial descritivo de software

8.4.1 Documento que deve descrever detalhadamente como os requisitos técnicos de software e hardware foram atendidos. A construção desse documento é abordada na norma de avaliação de software do respectivo instrumento.

Nota - Os documentos descritos no item 8.2 e 8.3, salvo o código fonte, podem ser anexados ao memorial descritivo de software.

8.5 Ferramentas

8.5.1 Ferramentas para verificação de integridade

8.5.1.1 Para cada software legalmente relevante o requerente deve incluir no pacote de entrega a correspondente ferramenta para verificação da integridade do software em campo, bem como seu procedimento detalhado de uso. Essa ferramenta é considerada legalmente relevante.

Nota - Se o instrumento possui interface de verificação metrológica, conforme especificado na Norma NIT-Sinst-020, não é necessário que o requerente forneça uma ferramenta de verificação.

8.5.2 Ferramenta para carga de software


8.5.2.1 Caso seja possível alterar o software legalmente relevante em campo sem romper a selagem principal, o requerente deve incluir as ferramentas para carga de software no pacote de entrega. Adicionalmente, deve incluir também arquivos que serão carregados como casos de teste para uma carga bem sucedida e uma carga mal sucedida. Essa ferramenta é considerada legalmente relevante.

8.5.3 Ferramenta para alteração de programa em instrumentos sem carga de software

8.5.3.1 Para evidenciar os requisitos de mudanças acidentais é necessário que o requerente prepare um binário modificado simulando uma alteração acidental. Caso o instrumento não possua carga de software, o requerente deve fornecer meios para a gravação desse binário no instrumento ou enviar um exemplar com o binário alterado.

8.6 Modificação de modelo

8.6.1 No caso do processo de avaliação de software ser relativo a modificação de um modelo já aprovado, deve-se adicionar um arquivo de diferenças ao pacote de entrega.

	NIT-SINST-003	REV. 01	PÁGINA 11/32
---	----------------------	--------------------	-------------------------

8.6.2 Arquivo de diferenças

8.6.2.1 Deve se redigir um documento textual esclarecendo as diferenças entre o software atual e o anterior. Caso o RTM requeira a entrega de arquivos de código fonte, deve constar nesse documento a diferença entre os arquivos do código fonte, quais arquivos foram acrescentados e quais removidos. Esse documento deve referenciar a portaria de aprovação de modelo anterior em seu início.

8.7 Casos de teste

8.7.1 O requerente deve entregar um documento de casos de testes, atestando a validação do software e do hardware do instrumento. Esse documento deve conter um conjunto de testes realizados comprovando o atendimento aos requisitos técnicos de software e hardware do RTM pertinente. Para cada caso de teste deve ser apresentado uma tabela contendo, ao menos, as informações apresentadas na tabela 1.

Tabela 1 - Exemplo de registro de caso de teste.


Item	Descrição
Título	Título do caso de teste.
Autor	Nome do responsável pela execução do teste.
Resumo	Contém uma descrição do caso de teste, descrevendo a finalidade ou o objetivo do teste e o escopo.
Pré-condições	Para cada condição de execução, descreve o estado obrigatório do sistema antes do início do teste.
Entradas	Para cada condição de execução, enumera uma lista dos estímulos específicos a serem aplicados durante o teste. Em geral, eles são denominados entradas do teste e incluem os objetos ou os campos de interação e os valores de dados específicos inseridos durante a execução deste caso de teste.
Procedimento	Para a execução do teste, são as ações que o usuário deve fazer para que o sistema possa cumprir com o que será testado.
Resultados encontrados	É o resultado da execução do teste. Observe que os resultados podem ser positivos e negativos.
Evidência dos resultados encontrados	Conjunto de informações que evidencia o resultado descrito no item anterior, tais como: <i>printscreen</i> da tela do sistema contendo o resultado, registro fotográfico ou gravação de vídeo, arquivo de log do sistema, bloco de dados trafegado como resposta, etc.
Pós-condições	Para cada condição de execução, descreve o estado ao qual o sistema deverá retornar para permitir a execução de testes subsequentes. Relatar somente em casos excepcionais.
Resultados esperados	É o estado resultante ou as condições observáveis esperadas como resultado da execução do teste. Observe que isso pode incluir respostas positivas e negativas (como condições de erro e falhas).

Fonte: Dimel/Disme/Sinst

9 PADRÃO DE ESTRUTURA DE DIRETÓRIOS

9.1 A seguinte estrutura de diretórios deve ser utilizada para organizar o pacote de entrega.

```
<raiz>/
  doc/
```

	NIT-SINST-003	REV. 01	PÁGINA 12/32
---	----------------------	--------------------	-------------------------

```

<modulo 1>/
  src/ // Códigos fontes do módulo 1
  bin/ // Binários
  lst/ // Listagens assembly
  lib/ // bibliotecas utilizadas
  int // ferramenta para verificação de integridade daquele módulo
  load // ferramentas para carga de software
  tools/ // Outras ferramentas
<modulo 2>
  ...
  ...
<modulo n>
  ...

```

9.2 Pasta <raiz>

A pasta raiz do pacote de entrega deve conter a pasta com os documentos para análise (./doc) e as pastas contendo as informações de software correspondentes a cada um dos módulos do instrumento (<módulo 1>, <módulo 2>, etc.). A contar da pasta raiz, não exceder a 256 caracteres (incluindo “/”) na formação do caminho. Esse limite é colocado para manter compatibilidade com Windows XP.

9.3 Pasta doc/

9.3.1 A pasta doc/ deve conter todas as documentações pertinentes a serem entregues pelo requerente, conforme descritos no item 8, salvo as ferramentas, descritas no item 8.5, e código fonte, descrito no item 8.3.5.

9.3.2 Caso o RTM requeira a entrega de arquivos de código fonte, os arquivos de código fonte e ferramentas devem ser colocados nas pastas específicas conforme descrito no item 9.4.

9.3.3 Opcionalmente, podem haver subdiretórios definidos pelo requerente de acordo com seu critério de organização, e, nesse caso, cada um desses subdiretórios da pasta documentação deve ser descrito num arquivo LEIAME.txt dentro da pasta doc/.

9.4 Pasta modulo_<modulo n>

9.4.1 Para cada software presente no instrumento deve ser criada uma pasta <modulo n>.


9.4.2 O nome <módulo n> deve ser substituído pelo nome ou por um mnemônico que melhor represente a funcionalidade do módulo em questão.

9.4.3 O nome da pasta <modulo n> não pode ser modificado de uma revisão para outra da documentação.

9.4.4 Cada pasta <modulo n> deve conter a documentação de um software referente ao módulo em questão. No caso de um instrumento monolítico, isto é, conter somente um módulo com software, deve ser criada também uma pasta <modulo n> correspondente ao único módulo presente no instrumento.

9.4.5 Dentro de cada módulo deve haver as seguintes pastas:

a) src – com o código fonte do módulo.

	NIT-SINST-003	REV. 01	PÁGINA 13/32
---	----------------------	--------------------	-------------------------

- b) bin – arquivos binários compilados do código fonte associado. O requerente deve fornecer um binário para evidenciar a falha de modificação acidental. Caso o módulo possua carga de software, o requerente deve fornecer arquivos binários extras para o ensaio funcional de carga de software. Nesse caso, deve haver um binário e sua respectiva assinatura digital para o qual o processo de carga de software falhe assim como um binário e sua respectiva assinatura digital para o qual o processo de carga de software seja bem sucedido.
- c) lst – listagens em *assembly*, caso necessário
- d) lib – bibliotecas utilizadas pelo módulo em questão, caso necessário.
- e) int – diretório contendo a ferramenta para verificação de integridade daquele módulo assim como o seu manual de uso.
- f) load – diretório contendo a ferramenta de carga de software daquele módulo assim como o seu manual de uso.
- g) tools – diretório contendo as ferramentas descritas no item 8.5 assim como quaisquer outras ferramentas que o requerente julgue pertinentes para que sejam realizados os ensaios funcionais, como por exemplo drivers para sistema operacional a fim de realizar comunicação com instrumento. Caso seja possível a gravação de programas na memória do instrumento, o requerente deve fornecer ferramentas para tal. (Por exemplo, para evidenciar os ensaios de modificação acidental.)

Nota - Caso vários módulos façam uso das mesmas ferramentas o requerente pode colocar a pasta tools na <raiz/> e reportar essa informação num arquivo texto pleno LEIAME.txt dentro da pasta tools.

10 REQUISITOS DE ASSINATURA DIGITAL

10.1 Caso o requerente faça uso de assinatura digital é necessário que ele preencha o FOR-Dimel-023 e especifique o algoritmo de assinatura digital e o algoritmo de hash criptográfico a ser utilizado.

10.1.1 O algoritmo de assinatura digital a ser utilizado deve ser dentre os algoritmos internacionalmente aceitos e documentados na FIPS 180 e FIPS 186.

10.2 No caso de uso de assinatura digital para carga de software remota, cada software aprovado no Inmetro deve ser assinado digitalmente com intuito de impedir que um software não aprovado seja carregado no instrumento de medição.


10.3 Existe ainda a possibilidade de uso de assinatura digital para boot seguro ou por requisito do RTM, como no caso de medidores de umidade de grãos.

10.4 Para cada algoritmo listado na FIPS 186 o Inmetro fornece uma chave de teste criptográfica para ser utilizada no processo de avaliação de software. O anexo C dessa norma apresenta uma chave teste para cada algoritmo aceito.

10.5 Para cada software daquele modelo que venha a passar no processo de avaliação de software, o requerente deve gerar uma assinatura digital de teste utilizando uma das chaves dispostas no Anexo C.

10.5.1 Para cada chave de teste é apresentado no anexo D um exemplo de assinatura digital.

10.6 A chave de teste e a assinatura digital de teste só devem ser utilizadas durante o processo de avaliação de software com intuito de verificar as funcionalidades de carga de software, boot seguro ou requisito do RTM (como no caso de medidores de umidade de grãos) do instrumento em questão.

	NIT-SINST-003	REV. 01	PÁGINA 14/32
---	----------------------	--------------------	-------------------------

10.7 Uma vez aprovado, o Inmetro deve gerar uma chave de produção e uma assinatura digital de produção. A assinatura digital gerada segue o padrão apresentado nos exemplos do anexo D.

Nota 1 - A relação entre modelo e chave criptográfica é de um para um. Cada modelo tem uma única chave de produção, essa chave não pode ser utilizada em outros modelos.

Nota 2 - A relação entre modelo e assinatura digital é de um para muitos.

11 RELATÓRIO DE ENSAIO DE LABORATÓRIO EXTERNO

11.1 O requerente pode utilizar de laboratórios acreditados ou laboratório da Dimci para realizar o ensaio de software.

11.2 Além dos requisitos da norma ABNT NBR ISO/IEC 17025 para apresentação de resultados, o relatório de ensaio de software deve conter:

11.2.1 Hash de identificação do pacote de entrega.

11.2.2 Versão/identificação do software: Número das versões/identificações de cada software legalmente relevante no instrumento que passou pela análise de software.

11.2.3 Nome(s) do(s) binário(s): Nome de cada arquivo binário legalmente relevante que passou pelo ensaio de software.

11.2.4 Hash(es) do(s) binário(s): Hash de cada arquivo binário legalmente relevante.


11.2.5 Algumas arquiteturas podem utilizar outros *hashes* para identificar o sistema. Esses *hashes* devem ser documentados no relatório de ensaio.

11.2.6 RTM do instrumento: O número da portaria que aprova o regulamento técnico metrológico e sua data de publicação devem constar no relatório de ensaio.


11.3 No anexo E é apresentado um exemplo de resultado do ensaio de software para um determinado item do regulamento técnico em questão.

12 HISTÓRICO DA REVISÃO E QUADRO DE APROVAÇÃO

Revisão	Data	Itens revisados
00	Mar/2018	<ul style="list-style-type: none"> ▪ Emissão inicial
01	Out/2018	<ul style="list-style-type: none"> ▪ Inclusão dos laboratórios acreditados no campo de aplicação ▪ Inclusão de prazo no envio da documentação por parte do requerente ▪ O item 10 foi reescrito. ▪ O item 11 foi adicionado. ▪ Várias alterações menores para melhor entendimento do texto

	NIT-SINST-003	REV. 01	PÁGINA 15/32
---	----------------------	--------------------	-------------------------

Quadro de aprovação		
	Nome	Atribuição
Revisado por:	Carlos Eduardo Cardoso Galhardo	Coordenador da qualidade do Sinst
	Fabiano de Oliveira Leitão	Pesquisador tecnologista em metrologia e qualidade
	Antônio Lacerda Junior	Pesquisador tecnologista em metrologia e qualidade
Verificado por:	Juliana Wilm Guedes	Estagiária do Sinst
	Amsterdam de J. S. M. de Mendonça	Coordenador da qualidade da Dimel
Aprovado por:	Bruno Erthal Abreu	Chefe do Sinst

	NIT-SINST-003	REV. 01	PÁGINA 16/32
---	----------------------	--------------------	-------------------------

ANEXO A - CHAVE PÚBLICA DO SINST

A-1. Para a troca segura de arquivos com o Sinst, deve-se utilizar criptografia através do software Gpg4win (para ambientes Windows) ou seu equivalente para outros ambientes, que pode ser acessado em <https://www.gnupg.org>.

A-2. A chave pública utilizada pelo Sinst é aqui detalhada:

```


-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2.0.22 (MingW32)

mQINBffup4ABEADe1KrAxYfYnCluieK2fWfcyTOW7OElm2mXpE9pxeGeKRZjZDSxy
5SIGX3ayTKh+2zedbTQ2R85xc7vUM7Jt74MY64JT/2T6pEprMAW9RrXJ4IsHKk34Q
TOo0M9TUvOmCUXvbadrnfzNXm17CQCpQ4nldfEEG7giZMY00FzuamapEUM4qZ2h
/eM0DQDiLqVxNLCIgpBI6ucbeEt/xqFtnG1i0Gqo5uXet8VYQOJbKbMZGEqIi7Mp
MeZPHbILp6JXzX2oerVxvucmn+F+XtWmVDNo/39y1ltg2YHlw6kAoI/noKZI6YP
KCM/fKTJ6tdKuFouJz8FJrsu9kVK8EDSQGMN5CPGbp4NN1U0m8P+1tCdD+8PAKFY
Dp9GCu/XsgsgIAXdh7W/Dhx/CakeR+YL6Qfhu8pfZEhy+gkpbMG60b/Zj/VmuU7
kOqifQE0BiLR/9usanUSsnS8c+mubjPBVnFQOnrbt313eEgQ2fxQpVADcE40PxdI
8EnLAdILuFqTQa1F2rGG/YZn3jYBBL2Zi+teJ6V0galjk4HMPXZPUj8Tfs9DVUDC
YQ+bohPb9VYFQoIuYgiSMMqq0K/87M1zdwXFt/YPkKJhG7cNJmH0/eIT8GtNjGf
eXAVSBxv85cJ/175ssflouSdvXwQnt9ZmH7Vfp0Uc05VpOZwPI3dPEgZhwARAQAB
tGtNYXJjb3MgVHJldm1zYW4gVmFzY29uY2VsbG9zICChDaGF2ZSBwYXJhIHRyYW5z
ZmVy6puY21hIHNlZ3VyYSBkZSBhcncFlaxZvcykgPG10dmFzY29uY2VsbG9zQGlu
bWV0cm8uZ292LmJyPokCPwQTAQIAKQUUCV+6ngAIBDwUJB/8x4AcLCQgHAWIBBhUI
AgkKCwQWAgMBAh4BAheAAAoJEBEG2H1eqVyIH10QANQwHK2mtlqXrNyO7AXE5q4v
9cRQvveMUEpbnz0uN+Q4IkxsDISjHFHSHffORmCbMSz/yPLJ76Rp1muWimUuJYs4
fgDwaC9Ma5P96so21xNhdXUWz3Mec2H1801J+dHIQ9MfBozv80UnKQCvBgBqxs7W
CZAPLqOF7NuCL4910VjGvsUzzvlp4kZ6GkiXN3cv7yrAxwDcY7ODPW8RMHardT6K
Fo0ioEPZW9GhmYIBKcM/OPwtZDfoOorHwQHfuMfUKzbDvxP15x6a6fvd54k2mRdS
N31Z0jKUTHc6H2nlfudo8z56udqjYCzH1hfRNP2tEg94G0guuE6Qubj7QBxwEu41
YDoAGxfn4t+H8DuDiId5+gL6udEG0vJxqybjZ1nGNghaE+9Bfx5D8XdFwn7Qxp9G
fdxHdcsL2SVcEbUdiPMYJjheuvlij6goly2vLwFnzFaZjiQzvt0yKO+6kDcoJUmp
ng2VMCEf5pGUIpa2z7mVcXGHnMQWYGIo16QFwn8R8BiRQ8eCE8KHmlAID7AvP+qh
zjnTy7DxEKadYVc8a065060ygnQN+Ayuvq7W/79hIK03f2RPODOqc5BhxGxTwnH
od4SoUbf9FY6ZjH0MB9ov3PrAZU2GeUCW/TGLycoQSSm+EbU2OejN01Y/YeWkmW
1UaBXJbDKHQ6qrLr5rkj
=6BuE
-----END PGP PUBLIC KEY BLOCK-----

```

A-3. Esta chave pode ser encontrada no site da Rede Nacional de Ensino e Pesquisa <http://www.rnp.br> em Início > Serviços > Serviços Avançados > ICPEdu > Servidor PGP, buscando-se por Marcos Trevisan Vasconcellos.

A-4. A chave é RSA 4096 bits, keyID 5EA95C88, criada em 30/09/2016, com validade até 31/12/2020.

	NIT-SINST-003	REV. 01	PÁGINA 17/32
---	---------------	------------	-----------------

ANEXO B – MODELO DE DECLARAÇÃO DE VÍNCULO

B-1. DECLARAÇÃO DO VÍNCULO ENTRE CÓDIGO FONTE LEGALMENTE ENTREGUE E O SOFTWARE EMBARCADO NO INSTRUMENTO

- (1) Nome e endereço da empresa: [Nome e endereço da empresa]
- (2) Nome do modelo: [Nome do modelo]
- (3) Código fonte e arquivos acessórios com seus identificadores: [Listagem ou referência a um anexo]
- (4) Programas executáveis juridicamente relevantes com seus identificadores: [Listagem ou referência a um anexo]
- (5) Data de geração: [Data]
- (6) Identificadores do modelo: [Listagem]
- (7) Forma como os dados foram enviados ao Inmetro: [Tipo de envio, ver item 7.1 dessa norma]

O abaixo-assinado declara que os programas executáveis legalmente relevantes listados em (4) no modelo especificado em (6), submetido para o processo de avaliação de software, foi gerado exclusivamente a partir do código fonte e arquivos de acessórios nomeados em (3), no suporte de dados indicado em (7).

[Lugar], [Data]

[Assinatura].

/ANEXO C



ANEXO C – PARÂMETROS DE DOMÍNIO PARA ECDSA

C-1. Parâmetro de domínio para curvas elípticas sobre corpos primos.

C-1.1. As curvas elípticas do tipo P são aquelas definidas sobre corpos primos com característica diferente de 2 e 3.

C-1.2. As curvas elípticas do tipo P possuem o seguinte formato: $y^2=x^3+Ax+B \pmod P$, em que P é um número primo e A e B são elementos do corpo.

C-1.3. Os pontos da curva formam um grupo aditivo.

C-1.4. O ponto G é um ponto da curva e também gerador do grupo, assim, Gx representa a abcissa do ponto G e Gy representa a ordenada do ponto G.

C-1.5. A ordem do grupo é representada por N.

C-1.6. Curvas recomendadas pelo NIST.

C-1.6.1. Curva NIST P-192


```
Nome: Curva NIST P-192
P = ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffeffffffffffffffffffffff
N = ffffffffffffffffffffffffffffffffffffff99def836146bc9b1b4d22831
A = fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffeffffffffffffffffffffffc
B = 64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1
Gx = 188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012
Gy = 07192b95fffc8da78631011ed6b24cdd573f977a11e794811
```

C-1.6.2. Curva NIST P-224

```
Nome: Curva NIST P-224
P = fffffffffffffffffffffffffffffffffffffffffffffffff00000000000000000000000000000001
N = ffffffffffffffffffffffffffffffffffffff16a2e0b8f03e13dd29455c5c2a3d
A = fffffffffffffffffffffffffffffffffffffffffffffffffffeffffffffffffffffffffffe
B = b4050a850c04b3abf54132565044b0b7d7bfd8ba270b39432355fffb4
Gx = b70e0cbd6bb4bf7f321390b94a03c1d356c21122343280d6115c1d21
Gy = bd376388b5f723fb4c22dfe6cd4375a05a07476444d5819985007e34
```

C-1.6.3. Curva NIST P-256

```
Nome: Curva NIST P-256
P = ffffffffff000000010000000000000000000000000000000000000000000000000000000000000000
N = ffffffffff00000000000000000000000000000000000000000000000000000000000000000000000000
A = ffffffffff0000000100000000000000000000000000000000000000000000000000000000000000000000
B = 5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
Gx = 6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
Gy = 4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
```

	NIT-SINST-003	REV. 01	PÁGINA 19/32
---	----------------------	--------------------	-------------------------

C-1.6.4. Curva NIST P-384

```
Nome:      Curva NIST P-384
P =        ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
           efffffffff000000000000000000000000000000000000000000000000000000000000
N =        fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffc7634d81f4372dd
           581a0db248b0a77aececl96accc52973
A =        ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
           ffffffffff000000000000000000000000000000000000000000000000000000000000
B =        b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875a
           c656398d8 a2ed19d2a85c8edd3ec2aef
Gx =       aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a38
           5502f25dbf55296c3a545e3872760ab7
Gy =       3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c0
           0a60b1ce1d7e819d7a431d7c90ea0e5f
```

C-1.6.5. Curva NIST P-521

```
Nome:      Curva NIST P-521
P =        1fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
           ffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
N =        1fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffa51
           868783bf2f966b7fcc0148f709a5d03bb5c9b8899c47aebb6fb71e91386409
A =        1fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff
           fffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffc
B =        051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156
           193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
Gx =       0c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa1
           4b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
Gy =       11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbdl7273e662c97
           ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
```

C-2. Parâmetro de domínio para curvas elípticas sobre corpos binários.

C-2.1. As curvas elípticas do tipo B são aquelas definidas sobre corpos com característica 2.

C-2.2. As curvas elípticas do tipo B possuem o seguinte formato: $y^2+xy=x^3+Ax^2+B \pmod{F}$, em que F é um polinômio irreduzível e A e B são elementos do corpo.


C-2.3. Por motivos de desempenho, o NIST adota um valor padrão para $A=1$.

C-2.4. Os pontos da curva formam um grupo aditivo.

C-2.5. O ponto G é um ponto da curva e também gerador do grupo, assim, Gx representa a abscissa do ponto G e Gy representa a ordenada do ponto G.

C-2.6. A ordem do grupo é representada por N.

C-2.7. Curvas elípticas do tipo B recomendadas pelo NIST.

	NIT-SINST-003	REV. 01	PÁGINA 21/32
---	----------------------	--------------------	-------------------------

C-3. Parâmetro de domínio para DSA:

C-3.1. O parâmetro P é um número inteiro positivo e primo.

C-3.2. O parâmetro Q é um número inteiro positivo e primo tal que Q divide (P-1).

C-3.3. Os elementos não nulos do corpo primo P formam um grupo comutativo multiplicativo H.

C-3.4. O parâmetro G é um elemento gerador do grupo H.

C-3.5. Inmetro DSA 160/1024 bits - 01


Nome: Inmetro DSA 160/1024 bits - 01

P = c862d38396851d29f12255cbd42e001dc5230d94f0426e29aa80a580075134a4
52efe519e901e2917c0ac92e5c1f93e41fd512bc9fa487a89b7fb910b0a91a65
cf8c901fb971bf82d531ad001ff7e563c78af5e9c705cc5d7cdcd22ded29b207
6817196c8735f3f9047a587c5a5577d066792304f2b30c41bf42ac8b77713cab
Q = e8c3e320fd0b271735113d1c42361b178ba77c1b
G = 9172a619115fd3af1047dcda207136433ebecd387b7ccf3dc88b9bcc03895f9d
cad2a7130f99542ed0d28af739b0b0249dd5f353153e9987e044e6e6e84fb7d5
c47c7bd39464d5d0674e6c527c8c61abac2247df002c16cf13f57321e0091057
082284ff8a0642ccc5a75120f65d1236fe8a943fb37e910b2bbd209283591a1b

C-3.6. Inmetro DSA 224/2048 bits - 01

Nome: Inmetro DSA 224/2048 bits - 01

P = 7ccealee4b96014e3b7faae45acdab64aeb1b44604aff896bb4520c4df7672d7
1f6b8f9da7e336624e1611492cb3c94723bb4eb20e257efa57e8c1c56c97eec4
15e4b724cf734ffb8e5b38aa3e0fa86ac931a74f3ba176c1ff003055a6faae69
098863eacdcebc891befcd236815f2dc385823b70bd251ea34324df51a154c6
5cf248189f9b85f296778ebce65dfd2334a9284453bfce05dfb6f92c2e926a33
baa93c10061c505ddeb6043197b839bb3c608dba908629965d600bb26705c433
f6ce08fd43a8c5125a51b66a7fb75f44c1dee5d1ab2bbb40f92419753f67c6ff
c15a7a45c5212e812fa7e098314727b7668530a898082aecb9bac813ecf68faf
Q = bc5dc507e61b94ceb91d5e5dae489a65600a15e2bd3617544500c3d9
G = 77fc882f674d66658eaddbf5925a8fa52791f250c41b4c3aafcd574e2b8a02e3
c5c6be132d40a5c6461026489159322358e7f8e2c21c0ab71c3f1d84a93828a6
2b362cfde39cc51bc4da9ce3450b7fc6ad75647e49c1854b1e97eb4ab51b0720
81dd5167866a0ae09800d2a926fae058e071590c1e2525cd84faa6d060e47dda
5d632bc7563ea691eacb512fa15ea56c33a8887abc700d23ca8cecea368a3c76
4f6676dbc46d1e734bb0e47ae8703b1591623adaf2772e6e615a6769f7a69a01
3608dfb13689953b4008e45bc8b1d97ec111bafa896dc77c010243127fdccf6a
d4c9e0500dcbd8e7884fae01cf353107e09efc0b1f6fffb0bbf7e13c85afc8988

	NIT-SINST-003	REV. 01	PÁGINA 22/32
---	----------------------	--------------------	-------------------------

C-3.7. Inmetro DSA 256/2048 bits - 01


Nome: Inmetro DSA 256/2048 bits - 01

P = a01a3df2a1f1157ce0e01dfc1b03ce0940414febbb3e1aed6dea4f89c1b1d43
d8d350cb2a541a9ac0f5208fc0aacbca5e9ac2317af21164e40515aed09523bf
173f1a8b1f57e8d10c32d58eb75c3ddfaac73f03fd3df170451dda3e971c1db3
74728ce4e87e2064bc5cf3cbf4f821f7e96974ee2f60129dee8c0a7aee14fd32
a9049bdb8c457df22c7cdd6f752d3d55ddce2d6603d8cf38727d33809284d77b
3e59d7ee914bd10c89d82b1acfd20fd207d30c10e8b3d94d7cbcb0fbb47007f
86eae1871bd82be601b2694e54d39bacbcf131eabc2b1a86ff211c67482f76b7
38906758b110ba87d09f377fc273206b930181f7f4740a63c342c6094fd7c827
Q = b6f531832115e2fc3499cf73300ffeb862afa9f3b0153a6231bcd42d4c5c8bed
G = 843fb96c4567a5a4689f2f873ce3ab2a1bfd7077e23212a5e426aa59b1c81303
8fb57028900d63714d7c1fd462b18e0e2088a88aa9a4a982e07eb4010378384a
f474b2f587d5d97e522124860b6bec1ae124e91fd22a871d83dcde7eaf4ca52
57a592660ca4f8ced15b9333e30b30f13925cc2d29f4bacf701b27676007cec0
9f0ff8c39940250ba0ce3a29e74268013a6261c8ee86b33fa0760006d225b2a0
ef1a10135612439d067d1824f189556c5af99c9d72dd7f37f8822d68dfaa77b5
a8bcaa981683f118f8f981afe94d6d33607d4d39c6980d95546f1f3ba10ee88b
26bc318a592296c66a0d64aa6604c1c24754c3c709266351fe4cec9f77ed7cac

C-3.8. Inmetro DSA 256/3072 bits - 01

Nome: Inmetro DSA 256/3072 bits - 01

P = 90bee1921995b71aaefc5663f82dd2619db78cb6b0ade997e8ca03a66b1fc5b0
a5b8fd23addab679557cea7a612b6e3ab9ee97ad1cf01d4f3f371383bcc2d6d1
0ec84611e5e67c6703b80e07cf7f34e1cdf217b2c7cd7facf197e173b0f5dbe3
a787ccf1c9e8b136cfd7d604f46d0bfb92be03fa5cda8de6445c9014d3651320
833f7e089839053cdeb733da10bd0ad95c96a79adff863949eaf173187d057d5
a7c69dc5f2e0d6a2fdaf887a6cbc7bfd9acd2173f030f77154ce508e16c5afee
0bf5b3715a46af71e34639f88a2c92153c5686476148146b69c435ff6377c7ad
8d9e3b157a1553d2f7212bac29d447391b8b9cb7b4c43eea6bbb781ebe197928
041a95451ec0c4c2f6973dcdcbccdf21881f0c020924ee9ce1cf6942821cbfff
df7137835d250c3282c327fd1c907a7b7578a5fb93dfbc17c9a0fc4f1713d22b
d9c61bb7974bd41377b1def7d97644ee727d47ba322cf315e8e5cf0463678ddd
93ec3c80920032418fa8dc9a433b8823f4948cdb5ddb3fe4a9f0947afb647fe7
Q = 932e4e064e8aa72369e0f8384d77d9afa8c1a9d6dc9e1db318e89900b91e5a79
G = 6bd4005aa443f9de39ab84f9903925bbb098d3df6cfd9809d8362b20c0ff459b
7c583351f30f3f1e60b762fd9ab57369c329f139c24502e71fab0c9838ef884
a8c7f3fa05cf531f6f5618448b9dab883c560efc0148371e02e9b074e0f003de
8a742f907a158198fef3588c4bafab8eb991f1e40856623dcf0f86523490b9e
716be10322bc80f6699c6d7eaceac5e3af00a328a41eb4c2f66987ac9894f5e44
9f1ab570f82e67cf54f5b95e120c9a0168373da5b21f7adc8201c2b38f470131
92417b0a4bf5f67a8cf47c09d90bfd7a29c0fdd67f56fbc9d26768fc861ffe0
fd17c37fd5114329ecd1fe1dddf3285a7a57574da969aef8b0b4aa62341bac9
d065dbb4e47cd8d1a9d82367944844d01881042875206dc43a058d2b03a9fe62
17fc7d924955ab0ab739c7b2800b82c4157ce6f26c89a332c5f3e04d22008870
a5005c1db5d97e7698223e4fcce69ee9ab59ecbb93d295787a425086fdcd8986
959b046f8f2f4e65ba4b24788eb5c0fcf7242456d578c8acca3574f71b02852c

	NIT-SINST-003	REV. 01	PÁGINA 23/32
---	----------------------	--------------------	-------------------------

ANEXO D – CHAVES PARA TESTE DE ASSINATURA DIGITAL

D-1. Chaves para algoritmo ECDSA.

D-1.1. Tanto para corpos de ordem prima quanto para corpos de ordem de potências de 2, o par de chaves criptográficas privada (D) e pública (X, Y) é definida como $D \times (G_x, G_y) = (X, Y)$.

D-1.2. ECDSA - Curva NIST P-192

D-1.2.1. Chave Privada

D = 6cb639e4a65cd40307f0594f7143794ebd91ae99c54d37e1

D-1.2.2. Chave Pública:

X = 2c18d22ef793617bce73fff49f8818581c806a65044b4e13

Y = 611de0f9965b4b8698f8b3e45e7e2793e25c3c82095c5706

D-1.3. ECDSA - Curva NIST P-224

D-1.3.1 Chave Privada:

D = e89328971496822c2dad0481d79dc9549f253296fb4763b9c30e5c2a

D-1.3.2 Chave Pública:

X = 4adc069c67fd6be3d3a9fb4a53e4fb42a83ca935563963bb2ec50d00

Y = be347d17041eca75a5fc2f668effedbc969b4a66a9cbd512b0565e3a

D-1.4. ECDSA - Curva NIST P-256

D-1.4.1 Chave Privada:

D = 992fa5098c1e5eec33d19cd27707a43097349a2899cc6459f401aba3abe4e6bf

D-1.4.2 Chave Pública:

X = d922d0b531c3538a6910e1a567e41aaf8a35da17d4907ffe4d66b354997c2b20

Y = 719580b51c9480eabdbb9a439bf3e68ff1225d97884e5d2098a6b0917881f462

D-1.5. ECDSA - Curva NIST P-384


D-1.5.1 Chave Privada:

D = 306d5ac687b76c8e03bb97b0e3b892b904797fe83772274e
109ce7443cb54524cf3c5f20f869a659140900a6adf0eab

D-1.5.2 Chave Pública:

X = affdb28efe892b26434c9dd9d7521dc30dd9e8138cbdd250
8c8d5aba018c264edbc7fb63a4ffd05e600f32b1399ea159

Y = a41e1f81c1a1bcb828247ffa383389e403798f8446c19733
1f1b7335959162f4a025b32b8d17dc524dff438c592ea92d

	NIT-SINST-003	REV. 01	PÁGINA 24/32
---	----------------------	--------------------	-------------------------

D-1.6. ECDSA - Curva NIST P-521

D-1.6.1 Chave Privada:

D = a6e2dd5807e5cb73d901308bba2a8e1e27e1bd65423e00a2efe2526a3cd9774b7
d2dfcbafc84edf09a29202b82e2cad16a21922c42598e70d0592b07434f2c376

D-1.6.2. Chave Pública:

X = 379587dbb2f5f91153d4c9a05e64b19a18a5089da2cee4344d36a8b0a789b4c2b
90b70adcaa78408cc7ac90236111494fb208fff2a915d05ebd972e5781a95f146
Y = 71620ba1b3c2368630b4d7c7281f8ec50d7f11465813753a4c83b74701ae43786
e2216f4a58de9cad77e707cdc0edefbf05135d65e342f9f1b373324010a8b99ad

D-1.7. ECDSA - Curva NIST B-163

D-1.7.1 Chave Privada:

D = 11b9b05cbe7d9936a62d4ba080aac316236afaa4c

D-1.7.2. Chave Pública:

X = 427e9f7651ea1bd2a5313a9d4cf5e02832aeb102c
Y = 4cb38c5dc47efe41c44a69f99f44e6ff7c0c6df9d

D-1.8. ECDSA - Curva NIST B-233

D-1.8.1 Chave Privada:

D = 88dfb0caa427edcf2d582899b5f9ce426efd84b3204f3328a90e3406972

D-1.8.2. Chave Pública:

X = 1d4dc1d5245f9f6c5f4c7e72a821dff5c6d2f3136972a7ab5c215a33b2
Y = 17f9297460147c2c0f4d54fdc67496f8750bfba9eb9b275559775fd7c9

D-1.9. ECDSA - Curva NIST B-283

D-1.9.1 Chave Privada:

D = 18d4941cca4fdf4c770998df5bb5961025fb6e5a85cdece77a614c780ddb17bc6ca44b1

D-1.9.2. Chave Pública:

X = 430e030f0964d364ea3de21fbaf8c62751d862dac1ffaf558cfe688361ca8e2a93ef64c
Y = 7acd5543c2508d19d3691a98a5896c3826b99c1f24f98ca82110db05ee45aa6934654b4


D-1.10. ECDSA - Curva NIST B-409

D-1.10.1 Chave Privada:

D = dd09d553da28e32573c41f3b2c33130becded3cace2607f91a2
8d1617f18a57e6338aec31a6fd4cc98edf89d94e377d46c9b55

D-1.10.2. Chave Pública:

X = 1a12152deb8094d2d1ab33e6d27d3f478a9bd50bc526a274bf5c
57a86c057a16fefaaafc08b3080236f5642ba4bd6d253baca4cb
Y = 18ffda9080842b65ec67bc85135102dee619b2f9702812d43cd6
71db4b857589196bc8d869c130884ef0588bbd99ba9be8933f5

	NIT-SINST-003	REV. 01	PÁGINA 25/32
---	----------------------	--------------------	-------------------------

D-1.11. ECDSA - Curva NIST B-571

D-1.11.1 Chave Privada:

D = 1d922c405da68a55993ca248a4a6c139a72f8e25f7c2fd2765ea16275a1d7275314963d4c268bf0f46c7e80a7c7e62c69c514b11cbca127c382610e6feba105f963be30f9e74d00

D-1.11.2. Chave Pública:

X = 195f5d62aa594235910059e4fcf03228d0b27c12f447664647ef374eab3ceca5c8dfa8965e74da4607227f06490332a3e8175a2fb50cba879ac5fab990e86a0a68cb685db5919fb
Y = 36fe965a6616111658cfbd069a97dc19034812dc996862d7d882741f4fffc0b755442f6a5b209e41a7b60276003a1f8609f54f6d27ededec73133bee4f8e7fef25659259e6c0ab09

D-2. Algoritmo RSA

D-2.1. Para o algoritmo RSA, uma mensagem M é assinada da seguinte forma: $M^{DE} \pmod{N}$, onde o expoente D é a chave privada e o expoente E juntamente com o módulo N formam a chave pública.

D-2.2. O módulo N é definido como o produto de dois números inteiros, P e Q, positivos e primos.

D-2.3. Chave para RSA-2048

D-2.3.1. Chave Privada:

D = 7cf66017a1efff62f0168e5f59522cd1a11168ca7054d0ad658341ea06bdb5fbc068b66746f4293889fab00eb19660ab1973bb8b09bb098cdc879e356c9c45500ab89dc04d3b1da42aa6f00ba2167050229bb114f25710f4e5cf1b5242e2c97a272210af15020aa3f21753873e427eb6def76e1a39343ff13e36df58719be19756937457896dd1d358755bf494b3f1ba7294cc19e67091204e466763b39ad7323ec9358f75d1dceb076762accc63fca367cc0905d686e454f16714110c39a1facbf320537c5c45a0a14f96083afd2d29779d940d9163283c7185ad7dc6ea5486be055b531619f0fb645461d2bafef111a51387701692e1f0727818c301a224ef81

D-2.3.2. Chave Pública:


N = 85676154490ec99c19afea60464ac96f286d58a312fd9fa701c5216bce7130bed91fd25cb74742e48ca12abc367b803a5278fb417f1de6c18bd21ca48e20f0376172bbb2809da732519f95af53990afd2698495e72580a9b31aa6c2112f5d7478ea7d74f5e7a0f29573b14bf1ba9d40158b359bdd99568069da714e57bd4ad984be0aeb2892e0f2f2855a58e64bb6086adc0790d08857ab64f7cfed6cc56b91088747fef4550cec70ed53a0f9e1548acd57f7eff8876d53b90c2d45189cf020d03e546c335d3473fd86a2372dcf75552919c7a0076521f1978ca8f7fe00cd28be9fee80ef7a82626f13afaf3c37700402baf5730ecfb3858b122fec614e76df

E = 10001

D-2.3.3 Complemento:

P = d05c9d599655b329757e48a4e1a0c4231879606ac9b70dfed7eaade09986df1f26b603f961436465e5b44a122ef68cf5586014e9f4b3d7ad2ca4e9d4189021205257d76327e3356fc6044902a0a40b794efe22dba9f94bdebb40734388e68f441ecdecde9f57f6d3aae141591389249501ef7d725db8b03e98c68546d9c9bf

Q = a3e77ccb3717f5feb0cd0b2a923910b520fbc18ede569f6edf779562a75ee188f6f5d07ff2bca5415c810f8be970ac525efa0565551771d777aa00dbdc21c4c9060c7f45d9b54209430def5a7e66e72b17c0ec4af4ee8e7f67818ff7919dfaf03eeb59deec139df399badf49a3e8fae5d2c1e81d26d44ad47662f6bfdcc95ae1

	NIT-SINST-003	REV. 01	PÁGINA 26/32
---	----------------------	--------------------	-------------------------

D-3 Algoritmo DSA

D-3.1. Com o algoritmo DSA, o par de chaves criptográficas pública e privada é definido como $E=G^D \pmod{P}$.

D-3.2. Inmetro DSA 160/1024 bits – 01

D-3.2.1 Chave Privada:

D = 92d4a6010a7950121a75e25e9d59b6328ed51a4a

D-3.2.2 Chave Pública:

E = 646d544fceb430cdd9a988af11b978813bdcc8861991eb2b65a542c8d4e97c89
a574269480ac6df91c0b4e6cea936c686a65667cf2231b75d1265620f661ab42
09868dd5d73a03227bd13d63335a384785ef21da5f361164d3feeb4875d78a69
f2881fe83f04a1dc6e54d0ab7e1690e6a79ab04df3c18e15a66f85b2eed9eab4

D-3.3. Inmetro DSA 224/2048 bits – 01

D-3.3.1. Chave Privada:

D = 458ef80bc8dfb7ea1d46ae93da37c21303004a9672f3a0b236336be

D-3.3.2. Chave Pública:

E = 142037b212db22e237e63a4335c88d557c4ca97586df22a129ceae4bc7df1951
1055518266c9108a9780a7544f92a5af72fc4b8aa82eae6828098b08a1b3e22e
5683fe2afe1c862e9cc132d5732caf3167b41c2244ba691cb61ba5b60a431a7c
41f958c06633150df4539cf467931bfe1f3c687d6b0a43b9b0245fc6c62cb528
baf88c54026e178c07936acbe80838c78efa2b25cd1669f33783524e945b2df1
0dcfc31309ac4795571fc6c0d0b07c6d536a54854a07d2f0c73914f4c71bc7ad
8ad7bea997768af1ee6661b466d7302282fd366c29ef1882259c22a62aee6883
bf809ff01b084ed9fe36069c3fddc03a6488ea86cfd525b35d2ccac1a78b48e4


D-3.4. Inmetro DSA 256/2048 bits – 01

D-3.4.1. Chave Privada:

D = 1f69e0eb5a8e5ab0a2bfff3c58a51462d9b4fd2bf3591479bf862d7ab479ee464

D-3.4.2. Chave Pública:

E = 81c19d82e0a2811c77e247feac9b442ad353b754ff014be54e12663e8926ff02
54c56192136beb67b64e0d843119dd1e7a3748c954db50610e028defa41d7c80
9935e1495ec39345b028e1f1329826844ff683e9805b280eb53cafb0a782e800
6329d1796b6629efef62872ac9f6206b67c536941c75d9ac7eec37c04c4bd650
98315d851bd74462cd18fb2f2f560b2a2d7f4d557fcff009585922ae21e2cac8
0d24609df082c10a0a5dee56e506b5dd4eaecf9ce6bf644048533b1c275dd853
3a70b242c7f881bbc2984826327e695ba784f5c2e2e0dfe4339a9ce07a343f23
bb63f663504534a74a0b573fb0a58689e87c7e6072c34a81d5d7222046cb0343

	NIT-SINST-003	REV. 01	PÁGINA 27/32
---	----------------------	--------------------	-------------------------


D-3.5. Inmetro DSA 256/3072 bits - 01

D-3.5.1. Chave Privada:

D = 808702033be09f3fc71b14580b42f136ae60ba430358249cb39bdd4ab58f620b

D-3.5.2. Chave Pública:

E = 4dfa44a7b8bd875151e52b8d9da976007c7766323ca9b74cfa33e6cccf55a8a1
f1065b0c3e23c9fe52926de59af046cc452f198bb27a5731990a27f55bf4804b
94ffd358fc5a52ee53af082253bf0c4371510d91ec061e36812551f35d7206e1
9af2055fe833f4f1db2787c86953e23a58ec3e6e712c443cfd4c5eaa159a6780
0093d833bccb2075633ed635ac35e11cfe7a36585ca82eeb61d1d2b0ea9317a6
f788a3badfb14899c89a3a9797b15af1efd290bffb4ee430b165041cda8d87c0
34efcb22ac703a3e7c083469ee0b0714f00d12e4633d634f3f6b11e641d9ab67
57ffd162243adaba51d78574c8c6780f5c2bacaace2eb6dded2b1d06287cadce
f05936162400cf36adf9258dee0897c637bfb4d1724c4ecd453271f348c67d88
9f97cdd69f58535b7b090909b06cc156fbec24abb7791b2b4e8bf8cf2cf6a09
f7812abcec154f035aba8d431486b5b4e538ba5852e538f0b289a09c8a6b5092
8f5f4b0cd3193a161ff10afc985db1992271b8b581779434c59f2828b7319ee2

	NIT-SINST-003	REV. 01	PÁGINA 28/32
---	----------------------	--------------------	-------------------------

ANEXO E – EXEMPLOS DE ASSINATURAS DIGITAIS PARA CHAVES CRIPTOGRÁFICAS DE TESTE

E-1. Esse anexo apresenta exemplos de assinaturas digitais geradas com as chaves de testes do Anexo C. Para todos os exemplos a seguir um arquivo binário (não é arquivo texto) com o seguinte conteúdo foi utilizado:

```
494180eed0951371bbaf0a850ef13679df49c1f13fe3770b6c13285bf3ad93dc
4ab018aab9139d74200808e9c55bf88300324cc697efeaa641d37f3acf72d8c9
7bff0182a35b940150c98a03ef41a3e1487440c923a988e53ca3ce883a2fb532
bb7441c122f1dc2f9d0b0bc07f26ba29a35cdf0da846a9d8eab405cbf8c8e77f
```

E-2. Esse arquivo binário deve possuir o seguinte hash (SHA-256):

```
4525b206c9203d1bddd77f7e46839d56467636720aee6efce35745ea6ec4ae51
```

E-3. Assinaturas digitais com as chaves do anexo D.

E-3.1. Inmetro DSA 160/1024 bits - 01

E-3.1.1. Chave da mensagem

```
K = ce705d7867226486b5878b7718c559fd42b474a2
```

E-3.1.2. Assinatura digital

```
R = 7127dec63165d3b9a6da06cfc04161eae72bf06
```

```
S = 91f04ba6768445ac64bc7bf849f6f200bb6da25a
```

E-3.2. Inmetro DSA 224/2048 bits - 01

E-3.2.1. Chave da mensagem

```
K = a7138f706b966b78277dff32d4eab3b31b50ed83cb67a0fb2feeb547
```

E-3.2.2. Assinatura digital

```
R = 4e3b85e3ca5a6d535d93d4d1d23cd3fb5728d64d5cbba6f42e4c9e43
```

```
S = 87d1314ce4068341518228602a76cf958847cd4a164e1eea2fbff9c8
```

E-3.3. Inmetro DSA 256/2048 bits - 01

E-3.3.1. Chave da mensagem

```
K = ae650b8fd36a1def6465443bd2f63c2fde73bb8a9f3dfb2f421a1f41de4da783
```

E-3.3.2. Assinatura digital

```
R = 905ba77ac925f90c8b90e8b0f9be3867e9335487d71830b120e8986276ece126
```

```
S = aaf15abb19112ef32bf55925610e39cac3659744c9de30fced90dfc568d1ac87
```

E-3.4. Inmetro DSA 256/3072 bits - 01


E-3.4.1. Chave da mensagem

```
K = 8bcd5bfb4b2f9164d6d2415c0bdd2c291bb7b0ff3e473afaa97d3b623481aa7d
```

E-3.4.2. Assinatura digital

```
R = 4bc919d6f04d778343121a3ca3198608f776504c847122898777defb1fd41471
```

```
S = 7166fd54f324e055074d25aa0c08b11c08cbd6cc801f99c43b786b3a471b9816
```

	NIT-SINST-003	REV. 01	PÁGINA 29/32
---	----------------------	--------------------	-------------------------

E-3.5. Curva NIST P-192

E-3.5.1. Chave da mensagem

K = bafad7f9904658b960a28c1c18885651ad3e31f9b8d56fe9

E-3.5.2. Assinatura digital

R = ba28970e3d97ba7963bf4be69f2905ef39cb04c89927adab

S = 86f6fe9564b1bf4deb82c844056433468e222778e385c326

E-3.6. Curva NIST P-224

E-3.6.1. Chave da mensagem

K = 96db9d078f1f44bea5697a13d027e40d5e69b7b54f11dcc701413833

E-3.6.2. Assinatura digital

R = 393a94c96aa95e02a90cf724bb6ffebab3e0fb257e2e8e11ef5f6c3c

S = 67d83d94da8e02b4aab26e628e005929c0308cafd2c2ebfcb2ed6df2

E-3.7. Curva NIST P-256

E-3.7.1. Chave da mensagem

K = 96bbc08f72fa5e6069c675cc7baee1afc413cb85d43e339d6d52157069741299

E-3.7.2. Assinatura digital

R = b82e088fdf2c0f0e2f8b555899538efb5b00a10f1057246b4c0fcf99e75bebe1

S = 4ab44f0b839b201d37bc0d81095a04875ecda06fadb7a3fb215dd57765ebe0db

E-3.8. Curva NIST P-384

E-3.8.1. Chave da mensagem

K = d5fe19012210923601c8cbb9206883165fd0e5f53f42dfcb
00cca2949071255beda775b7a200777d550dc6d3bacce21e

E-3.8.2. Assinatura digital

R = 64dba15e9f6d71b272a9996f17313c29fcbbbaab618cfc2f
040e74fa2c1a98f19dcc083dacc650652162b24d386fed

S = d5db8afd0169096058eb0c5477bfcb81357a44a8959b013e
fe8d60f8e221177e278f392bb2f1f8e0ffe56b91e28dbc75

E-3.9. Curva NIST P-521


E-3.9.1. Chave da mensagem

K = 11ad6d658a42e0ca162b2ec1f3ed7b8cb4091123abfa3bb28a8cdcdfb7ec19bcbe
51aa2ed43f801c1dc9f8d850b840ec38459ae142369df667655c635fd3bd392

E-3.9.2. Assinatura digital

R = 03fc53760efdd4af0c94f85a3e03e26f58e2249400aac67bc3fd0103b12e255658
34b009bdbac26c31a617164420da4011932d3e8fb8605d450a51cd36c7d267b1e

S = 10cfc6963e1c70e4df7798e6a594f8f8966afdad777eb7a3a54826c9a71547b6ef
b8a6d1094a94486d475a96997593ae1200f2e501f03cdde3108da85b479756d32

	NIT-SINST-003	REV. 01	PÁGINA 30/32
---	----------------------	--------------------	-------------------------

E-3.10 Curva NIST B-163

E-3.10.1. Chave da mensagem

K = 35f18d7dcd627055c9835821048ccce0048ca095f

E-3.10.2. Assinatura digital

R = 03f03b63d0fed8af0abae40ce0c20cd3c19248c77

S = 3c7a030ca222befcdafc104e0b242816247c46fde

E-3.11 Curva NIST B-233

E-3.11.1. Chave da mensagem

K = ea48b688ba17f862b0cb91f27d1851b59ba70cb0a67e5c130c72c46a89

E-3.11.2. Assinatura digital

R = 09196701d457cbdbc22af759309101e5823de0cfc95e5a41092b654b4bd

S = 017f2d485bec51cc2b0adf4620c6876c5c817b9e8b0f7860c134e2faa15

E-3.12 Curva NIST B-283

E-3.12.1. Chave da mensagem

K = 14d5e1e064ffc796ede82376e6a10c35721f4641cd3871c088cf1367b58b19ad206d529

E-3.12.2. Assinatura digital

R = 2c71576482c357f144c1f01ee705bca821f9a109fd2d2c782a2cd51a20a5c53fc679be0

S = 2205d6e6eb655999edd175c410fda9f9b09649803f7859d39204dfed06a85b5735f8a01

E-3.13 Curva NIST B-409

E-3.13.1. Chave da mensagem

K = fae89b41bba663396058ff1e777f596ffecbf0b6360524651a8
d001cd43cb8930159e64568110a6e785edb70eefd915b178e8f

E-3.13.2. Assinatura digital

R = 0c4b9c920adefc610e3b2cc9932764b28ed9576b7100398bac80

a7eaa7fe6f36390c623d7dd3cca165e6579baafd2e5270ea3f2

S = 0829dba9a68fef5160d7244003df759d4252a6bb9b096f6fb70d

b35b179b84f43230a049f1890ee30603cf82b62dfac59f95b40

E-3.14 Curva NIST B-571

E-3.14.1. Chave da mensagem


K = 140ae32a8dab2593b05aa4c7c28f3f7b8416741683bea44891af354ac7cf0e4b5e0ab410
1a1661a690c1c7f622dba8b065e27f863e17c9d0cf3e36060107b8215c0085c1d9917b1

E-3.14.2. Assinatura digital

R = 100884385859173f2d1ef473862f1d343233849b13554c86cc505d3236e51f1044865284
8b13289a589a4e1778fa90c0237fbaf22b24bc4c745b084116fd4463f1ab5a4c0e590ec

S = 14bf7a6ce150de6a14116dea440bc8ffa2c38c840749a51fel8bf6b4c4af7b51fcfa084
d942627b99d9530ee44317fdbb595412f57dc7b537636b5744d15621d4a97b9f449199d

E-3.15 RSA-PKCS

	NIT-SINST-003	REV. 01	PÁGINA 31/32
---	----------------------	--------------------	-------------------------

E-3.15.1. Assinatura digital

46338da9ece399666baf21c0b0c3f6f989a4c16bdae9591cdb96db5bbd89d62c
ec1d89fcaeb1b74dfd4b32f213f510a67e948c34188112cff5eb91f439a727ebf
8e903d5ff928843d4df808ab63a0682c043b544c2c111b28cb78be5f270c1f95
4e5616fa5bd2ba38db0a73658ff19730a70fd31de01425ab681a1dcaf8d1ed70
98b0faa6612e53fdc9ca2fa55952d6857676cecd01c149e9bea867674c8895b4
73cb8645d016a13960f37d08077225c7a4e52897937c155bcb64e65cb9b0c1e6
69045fd6298b1326124b244ac3821ca2322ea39f6a8f4db8c27be8e50f4ce86e
1400b6f8e1a61b88aab393684f83a14124970fa2b41ded288fa965a6925722c7


E-3.16 RSA-PSS

E-3.16.1 Valor do *salt*:

a2be695ab3fde8ccbbd48ca4afa8d17ad4c1c717

E-3.16.2 Assinatura digital:

4186938187fe7991c359a02804dd14d0530bdae90707a9a35485177442586bea
bcba781306b092c57d792747e6d7b399e6534a1d5348f968084cb0bc884fe08d
c7514b77c64a3fc430116027d38c169648f29ffd8bd91758ebb53e88cf867e7b
ab06817218ac53a632de6047f5c11c285c380551a1454059bc63bbd6cc903fd8
a8f83d23a4d3e6636e06408589a61c3c9e9bf58fed16f8d0f26305fc630cd508
b6db9e3b51b0cbc82438735c482f6c70768236994e5b2e19209e85f72719be89
92168c25173747e17268e738c9a2b1ac8a6eb607389c75dcd20737877abafae2
266d9012fc7428a8fa3d3deb43612ab2b2d8077c22975c49a95a6f0b0a723440

	NIT-SINST-003	REV. 01	PÁGINA 32/32
---	----------------------	--------------------	-------------------------

ANEXO F - EXEMPLO DE PROCEDIMENTO, RESULTADO E CONCLUSÃO PARA RELATÓRIO DE ENSAIO

Tabela 2 – Exemplo do procedimento, resultado e conclusão para relatório de ensaio

Item do regulamento	Integridade de software (3.1.2)
Procedimento:	Utilizar a ferramenta disponibilizada pelo requerente e realizar ao menos 10 verificações de integridade que cubram toda a faixa de memória de programa. Explorar resultados positivos, usando como base o binário correto, e resultados negativos, utilizando como base um binário incorreto.
Resultado:	A verificação de integridade de toda a memória foi realizada a partir de intervalos disjuntos de tamanhos aleatórios. Um total de 100 réplicas foi realizado. Um teste de resultado negativo, utilizando um firmware modificado foi realizado. Todos os resultados corresponderam ao esperado.
Conclusão	Conforme

Fonte: Dimel/Disme/Sinst

Z