INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO - ITI
DIRETORIA DE AUDITORIA, FISCALIZAÇÃO E NORMALIZAÇÃO
COORDENAÇÃO-GERAL DE NORMALIZAÇÃO E PESQUISA

Nota Técnica nº 003/2016 – CGNP/ITI

Esclarecimento sobre alterações nas Políticas de Assinatura e sobre as atualizações nas Listas de Políticas de Assinatura Aprovadas no âmbito da ICP-Brasil.

O INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO - ITI, Autarquia Federal, na qualidade de Autoridade Certificadora Raiz – AC Raiz da Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, pelo conduto da Coordenação-Geral de Normalização e Pesquisa, subordinada à Diretoria de Auditoria, Fiscalização e Normalização, vem a público esclarecer que:

Esta nota técnica tem como objetivo reforçar a informação apresentada na Nota Técnica n° 1/2016 - CGNP/ITI, publicada em 1° de junho de 2016, que apresentou esclarecimentos sobre um novo conjunto de artefatos de assinatura digital, que tratam a nova cadeia de certificação da AC Raiz, a cadeia V5, e implementam melhorias apontadas pelo grupo permanente de trabalho que trata do Padrão Brasileiro de Assinatura Digital, o GT PBAD.

Na ocasião, foram disponibilizadas as primeiras versões das políticas PAdES e da respectiva Lista de Políticas de Assinatura Aprovadas - LPA, bem como novas versões das Políticas CAdES e XAdES. No caso dos Padrões CAdES e XAdES, foram feitos ajustes na codificação da LPA com o objetivo de refletir integralmente a versão textual disponível no DOC-ICP-15.03.

Adicionalmente, para facilitar a organização, as LPA receberam nomes de fácil associação com o padrão que representam. Desta forma, o arquivo da LPA do padrão CAdES passou a ser nomeado como LPA_CAdES.der, a LPA do padrão PAdES recebeu o nome de LPA_PAdES.der e neste mesmo contexto a LPA XAdES recebeu o nome de LPA_XAdES.xml. Todos os arquivos estão na versão 2 da LPA, visto que a LPA versão 1 foi descontinuada.

Considerado um necessário período de transitoriedade para que as aplicações legadas possam ser ajustadas para uso das novas LPA corrigidas e renomeadas, as LPAv2, tanto na codificação ASN.1 quanto na XML, estão sendo mantidas inalteradas por 2 (dois) ciclos de LPA, contados a partir de 01/06/2016.

Da mesma forma, a versão 2.2 de todas as Políticas de Assinatura XAdES e a versão 2.1 das Políticas CAdES AD-RB, AD-RT, AD-RV e AD-RC, bem como a versão 2.2 da Política CAdES AD-RA, serão mantidas por estes mesmos dois ciclos.

Assim, com a chegada ao final do primeiro ciclo, em 30/08/2016, deve-se observar que ainda há mais um ciclo, noventa dias, para que as aplicações legadas possam ser ajustadas para utilizarem estes novos artefatos (Políticas de Assinatura-PA e Lista de Políticas de Assinatura Aprovadas-LPA).

Em 28/11/2016, final do prazo de transitoriedade, as Políticas de Assinatura mencionadas no sexto parágrafo serão revogadas e os arquivos identificados com LPAv2 serão descontinuados.

Brasília, 29 de agosto de 2016

WILSON ROBERTO HIRATA:52049094949

Assinado de forma digital por WILSON ROBERTO HIRATA:52049094949
Dados: 2016.08.30 16:07:12 -03'00'

Wilson Roberto Hirata
Coordenação-Geral de Normalização e Pesquisa