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

Nota Técnica nº 001/2016 – CGNP/ITI

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

O INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO - ITI, Autarquia Federal vinculada ao Ministério da Ciência, Tecnologia, Inovações e Comunicações, 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:

O ITI emitiu uma nova cadeia de certificação da AC Raiz, a cadeia V5, em 02/03/2016, conforme publicado no sítio do ITI.

Ato subsequente à emissão de uma nova cadeia de certificação da AC Raiz, o ITI está emitindo novas Políticas de Assinatura (PA) contemplando essa nova âncora de confiança em suas regras.

As novas versões dessas políticas contemplam correções necessárias nos formatos CAdES e XAdES e ainda na versão textual das PA, descritas no documento DOC-ICP-15.03. Essas atualizações são resultantes do esforço dedicado do Grupo de Trabalho Permanente de Revisão do Padrão Brasileiro de Assinaturas Digitais (GT PBAD), sob demanda do Comitê Gestor da ICP-Brasil.

Foi ainda incorporada às novas PA, a previsão de uso do algoritmo SHA512 nas suítes de assinaturas digitais. Além disso, o ITI está lançando as PA em código de máquina para o formato PAdES ICP-Brasil, somando-se aos formatos já disponibilizados para CAdES e XAdES, padrão ICP-Brasil.

Quanto às Listas de Políticas de Assinatura Aprovadas (LPA), em decorrência das correções necessárias e dos novos componentes que passaram a integrar o arcabouço das assinaturas digitais ICP-Brasil, o ITI está disponibilizando nova apresentação de publicação das LPA no repositório da AC Raiz.

Nessa nova apresentação, mantém-se a primeira versão das LPA codificadas em ASN.1 e XML, porém, encontram-se descontinuadas, ou seja, somente para valor histórico, não entrando na vigência do ciclo corrente de LPA.

As LPAv2, tanto na codificação ASN.1 quanto na XML, serão mantidas inalteradas pelos próximos 2 (dois) ciclos de LPA, ou seja, até 28/11/2016, considerado como período de transitoriedade para que as aplicações legadas possam ser ajustadas para uso das novas LPA corrigidas e renomeadas em decorrência da entrada do formato PAdES.

Desta forma, novas LPA foram disponibilizadas com todas as atualizações descritas neste documento e passam a ser identificadas com a seguinte nomenclatura:

- LPA_CAdES.der

- LPA_XAdES.xml

- LPA_PAdES.der

Vale destacar também que as PA em CAdES e XAdES em suas versões que sofreram correções serão mantidas vigentes pelos próximos 2 (dois) ciclos de LPA, ou seja, até 28/11/2016, em período de transitoriedade, para que as aplicações legadas possam ser ajustadas para utilizarem as versões mais recentes das PA.

Brasília, 1º de junho de 2016

Wilson Roberto Hirata
Coordenação-Geral de Normalização e Pesquisa