INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO - ITI
DIRETORIA DE INFRAESTRUTURA DE CHAVES PÚBLICAS
COORDENAÇÃO-GERAL DE OPERAÇÕES

Nota Técnica nº 07/2017-CGO/DINFRA/ITI

Recomendação para uso de Certificados Digitais SSL da cadeia AC-RAIZ V2"

Em recentes levantamentos sobre os navegadores com mais uso na Internet do Brasil, os números indicaram que 86% dos ambientes empregam produtos (Google Chrome, Microsoft Internet Explorer e Edge) que utilizam o repositório de certificados confiáveis do próprio sistema operacional, predominantemente – 90% dos casos – Microsoft Windows em suas várias versões.

O ITI mantém tratativas para inclusão dos certificados raízes da ICP-Brasil nos repositórios de certificados confiáveis dos fabricantes e desenvolvedores de sistemas operacionais e navegadores como Microsoft, Google, Apple, Adobe e, inclusive, Mozilla. Tal iniciativa tem por objetivo evitar as mensagens de alertas de segurança que são apresentadas ao visitar sítios que possuem certificados digitais não inseridos nestes repositórios, causando transtornos para os usuários finais.

Um exemplo é a cadeia V2 da ICP-Brasil já inserida no sistema Microsoft Windows, estando em andamento tratativas para a inserção do certificado raiz da cadeia V5.

Iniciado o ano de 2017, grandes *players* da Internet passaram a exigir que a emissão de certificados digitais fosse feita em autoridades certificadoras que tratassem separadamente os casos de uso SSL, SMIME, CODESIGNING ou TIMESTAMPING. A ICP-Brasil, por sua vez, tornou obrigatória tal separação, nas suas cadeias V2 e V5, por meio do DOC-ICP-01.02.

Vale esclarecer que a cadeia de certificação V5 emprega os mesmos algoritmos criptográficos da cadeia V2, diferenciando-se exclusivamente por possuir maiores prazos de validade nos certificados das Autoridades Certificadoras subordinadas.

No que tange ao uso de certificados digitais ICP-Brasil, conforme dita o Decreto nº. 3.996 de 31/10/2001:

> *"Os serviços de certificação digital a serem prestados, credenciados ou contratados pelos órgãos e entidades integrantes da Administração Pública Federal deverão ser providos no âmbito da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil".*

Dado o exposto o ITI recomenda que órgãos e entidades da Administração Pública Federal, para evitar mensagens de alerta de segurança eventualmente postadas aos cidadãos quando do acesso às suas páginas, utilizem em seus sítios certificados SSL emitidos na cadeia V2 por AC habilitadas e, portanto, caso existam sítios atualmente usando certificados da cadeia V5, que seja realizada a troca.

ANDRÉ MACHADO CARICATTI
Coordenador-Geral de Operações