Alteração nas Condições de Confiabilidade das Políticas de Assinatura ICP-Brasil

O Instituto Nacional de Tecnologia da Informação – ITI abre a toda sociedade Consulta Pública sobre mudanças nas Políticas de Assinatura. A mudança implica em alteração nas Condições de Confiabilidade dos Certificados ICP-Brasil.

A ICP-Brasil define um conjunto de condições de confiabilidade para os certificados que são utilizados para a geração de assinaturas digitais e carimbos do tempo. Estas definições estão nas Políticas de Assinatura descritas no anexo 2 do DOC-ICP-15.03, tratadas no item 5.2.1 em cada Política de Assinatura.

Entre essas condições estão os Conjuntos de Políticas de Certificado Aceitáveis, onde constam os OID das políticas de certificado que podem ser aceitas em cada propósito, assinatura ou carimbo, e para cada tipo de certificado digital (A1, A2, A3, A4, T3 e T4), conforme o caso. Atualmente, este conjunto de política está implementado como uma lista, com um intervalo de 0 a 100, dentro de cada Política de Assinatura ICP-Brasil.

Ocorre que em 2016, em função dos requisitos adicionais para aderência aos programas de raízes confiáveis, tratadas pelas Instruções Normativas 07/2016 e 12/2016, houve um aumento significativo no número de Autoridades Certificadoras na ICP-Brasil e consequentemente de novas políticas de certificado. Atualmente, o número de políticas de certificado está muito próximo do limite estabelecido nas configurações das políticas de assinatura. Acredita-se que o intervalo disponível ainda suporte o credenciamento de AC previsto para 2017, mas é preciso estabelecer uma solução imediatamente.

A questão foi levada para discussão em Grupo de Trabalho, onde foram apontadas três alternativas de solução:

1. Aumentar o intervalo previsto para essas políticas de certificado dentro das políticas de assinatura.

2. Remover os conjuntos de políticas de certificado aceitáveis de dentro das políticas de assinatura, tanto para assinatura quanto para carimbos do tempo.

3. Manter o conjunto de políticas de certificado aceitáveis apenas para carimbos do tempo.

As três soluções são viáveis e apresentam prós e contras que devem ser considerados:

1. O aumento do intervalo é uma solução imediata, mas apenas adia o problema. Além disso, essa lista de políticas de certificado ocupa mais de 90% do tamanho de um arquivo de política de assinatura, logo, o aumento da lista aumenta proporcionalmente o tamanho dos arquivos de política de assinatura.

2. Com a remoção do conjunto de políticas de certificado aceitáveis, as aplicações não teriam mais como verificar se a política de certificado associada ao certificado digital permite seu uso para assinatura digital ou para assinatura de carimbo do tempo. Essa validação teria que ser feita pela verificação do propósito de uso do certificado.

3. A manutenção do conjunto de políticas de certificados aceitáveis apenas para carimbo do tempo aponta uma solução intermediária entre as duas primeiras soluções.

Deve-se observar que na adoção de qualquer uma das alternativas apontadas serão necessárias novas versões de todas as políticas de assinaturas previstas na ICP-Brasil. Para minimizar possíveis impactos em sistemas de informação, essas políticas são alteradas no máximo uma vez ao ano, estando a próxima alteração prevista para 27/05/2017.

Com o objetivo de ouvir a comunidade interveniente em assinaturas digitais ICP-Brasil sobre essas questões, o ITI manterá esta consulta pública aberta no período de **01 de março à 28 de abril de 2017**. Para enviar sua opinião, suas experiências ou outras informações que possam contribuir com esta importante decisão, acesse o formulário Consulta Pública - Condições de Confiabilidade dos Certificados ICP-Brasil.