

Pauta 05

Autorização à AC RAIZ para emissão de novos certificados Raiz v12 (S/MIME) e Raiz v13 (Passaporte Eletrônico) e atualização de seus Prestadores de Serviço de Suporte - PSS

1. Síntese do problema ou da situação que reclama providências

1.1 Novos certificados Raiz v12 (S/MIME) e Raiz v13 (Passaporte Eletrônico)

O certificado raiz v5 da ICP-Brasil, cadeia destinada à emissão de certificados digitais para assinatura de documentos e transações eletrônicas (tipo S/MIME), terá o fim de sua vigência em 02 de março de 2029, enquanto o certificado raiz v4 da ICP-Brasil, cadeia destinada à emissão de certificados digitais para assinatura de passaportes eletrônicos (curva *Brainpool*), terá o fim de sua vigência no dia 23 de abril de 2035.

O DOC-ICP-04, versão 8.1, em seu item 6.3.2.3, define os períodos máximos de validade para os certificados ICP-Brasil, conforme o tipo de certificado. Temos então o prazo máximo de validade dos certificados da raiz v5 de 6 (seis) anos para certificados dos tipos A4/S4/T4, e de 5 (cinco) anos para certificados do tipo A3/S3/T3 e A CF-e-SAT. No caso das cadeias hierárquicas em Curvas Elípticas, como a raiz v4 (*Brainpool*), temos o prazo máximo de validade de 11 (onze) anos para os certificados dos tipos A4/S4/T4.

O DOC-ICP-05, versão 6.3, em seu item 4.1.2.2, alínea 'w', define que as AC não podem emitir certificados com prazo de validade que se estenda além do prazo de validade de seu próprio certificado. No item 6.3.2.4, o DOC-ICP-05 estabelece que a validade admitida para certificados de AC é limitada à validade do certificado de AC que o emitiu. Já o DOC-ICP-01, versão 6.0, item 7.1, alínea 'b', define que o certificado de AC de nível subsequente ao da AC Raiz possui validade limitada à validade do certificado da AC Raiz.

Portanto, a partir dos normativos citados, depreende-se que o prazo de validade para todos os certificados emitidos sob uma determinada raiz ICP-Brasil está limitado ao prazo de validade do certificado raiz daquela cadeia. No caso concreto, todos certificados emitidos sob a cadeia v5 da ICP-Brasil têm, portanto, com prazo máximo de validade a data de 02 de março de 2029 e todos os certificados emitidos sob a cadeia v4 da ICP-Brasil têm com prazo máximo de validade a data de 23 de abril de 2035.

Por conta das regras acima descritas, os certificados dos tipos A4/S4/T4 da cadeia v5, hoje, já não podem ser emitidos com seu prazo máximo de validade (6 anos), visto que, desde 02 de março de 2023, ultrapassariam o prazo de validade da raiz v5 (02/03/2029). O mesmo ocorre com os certificados dos tipos A3/S3/T3 e A CF-e-SAT, estando impedidos de serem emitidos com seu prazo máximo de validade (5 anos).

Quanto aos certificados dos tipos A4/S4/T4 da cadeia v4, desde 23 de abril de 2024, estão impedidos de serem emitidos com seu prazo máximo de validade (11 anos), visto que ultrapassariam o prazo de validade da raiz v4 (23/04/2035).

Isso posto, faz-se necessária a emissão de novas raízes ICP-Brasil (v12 S/MIME e v13 Passaporte Eletrônico), o que proporcionará a continuidade de emissão de certificados ICP-Brasil dos tipos A4/S4/T4, A3/S3/T3 e A CF-e-SAT com seus prazos máximos de validade conforme regulamentado. As novas raízes devem figurar no rol de certificados raízes da ICP-Brasil, em sua Declaração de Práticas de Certificação – DPC (DOC-ICP-01).

1.2 Atualização dos Prestadores de Serviço de Suporte – PSS da AC Raiz

A operação da AC Raiz requer redundância do ambiente seguro de alta disponibilidade, alocação de hardwares e softwares criptográficos, serviços e suporte necessários ao desempenho das suas funções de acordo com as especificações estabelecidas pelas normas e práticas específicas. Nesse sentido, o ITI mantinha acordo com a Universidade Federal de Santa Catarina - UFSC para atuar como PSS para a disponibilização de infraestrutura física e lógica e de recursos humanos especializados para o ambiente de contingência da AC Raiz da ICP-Brasil.

Incluía-se no rol de responsabilidades do referido acordo com a UFSC o provimento, a administração e a manutenção dos meios necessários à operacionalização da Autoridade Certificadora Raiz - AC Raiz e da Entidade de Auditoria do Tempo - EAT da ICP -Brasil.

Com a finalização do acordo com o PSS UFSC da AC Raiz para o ambiente de contingência, em 30 de junho de 2024, e a contratação de um novo PSS para tal finalidade, fica evidenciado que a indicação nominal desse ente na DPC da AC Raiz pode ficar em desacordo com o que está sendo praticado, uma vez que sua alteração depende de uma reunião do Colegiado, sendo necessário um mecanismo de atualização dessas informações de forma mais simplificada e tempestiva.

2. Soluções e providências contidas no ato normativo

Resolução do Comitê Gestor de alteração na Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-Brasil (DPC da AC Raiz, DOC-ICP-01) para incluir as novas raízes v12 e v13 no rol de certificados raízes da ICP-Brasil e para tornar a atualização das informações sobre o PSS mais simplificada e tempestiva, remetendo a sua especificação para o repositório da AC Raiz.

3. Alternativas existentes às medidas propostas

Não há alternativas existentes à medida ora proposta.

4. Custos

Quanto à emissão e manutenção de certificados raízes e certificados de AC subsequentes à AC Raiz, no âmbito da AC Raiz incorre-se nos custos usuais de operação.

Para as AC subsequentes à AC Raiz, que desejarem vincular-se às novas cadeias, aplicar-se-á a cobrança de tarifa de emissão de certificado pela AC Raiz, conforme estabelecido no DOC-ICP-06, versão 4.0, item 1.2, alínea 'b', respeitadas as exceções estabelecidas no item 1.4 do mesmo documento.

As AC incorrerão, ainda, em seus custos operacionais usuais para a emissão e manutenção de seus próprios certificados e de certificados por elas emitidos.

5. Razões que justificam a urgência

A urgência para a aprovação ora pleiteada se justifica pela necessidade de a AC Raiz ter a devida autorização do Comitê Gestor da ICP-Brasil para que possa adotar as medidas administrativas e operacionais necessárias para a emissão dessas novas raízes, de modo a viabilizar a operação a tempo de minimizar o impacto sobre prazos máximos de validade dos certificados do tipo A3/S3/T3 e A CF-e-SAT, os de maior emissão atualmente, a partir de 02 de março de 2024, bem como de minimizar o

impacto sobre os prazos máximos de validade dos certificados do tipo A4/S4/T4 que servem, entre outras coisas, para assinatura dos passaportes eletrônicos do Brasil.

6. Impacto/Riscos sobre as operações da ICP-Brasil

A não autorização pelo Comitê Gestor do ora pleiteado impactará os prazos de validade máximos dos certificados já citados, emitidos sob as raízes atuais, v4 e v5, de modo que serão sucessivamente menores até o limite de 02 de março de 2029 e 23 de abril de 2035, respectivamente. No caso específico dos passaportes eletrônicos brasileiros, a não emissão de uma nova raiz implicará na impossibilidade de emissão de passaportes eletrônicos a partir de abril de 2025.

7. Análise de Impacto Regulatório

Considerando que é imperativa a geração de novas cadeias (v12 e v13) da AC Raiz para permitir a continuidade da emissão de certificados digitais com os prazos de validade determinados pela ICP-Brasil, bem como para regular a mandatória manutenção das instalações de infraestrutura de contingência da Autoridade Certificadora Raiz, entende-se que a pauta em questão se enquadra em caso de dispensa de AIR, de acordo com os incisos II e IV do art. 4º do Decreto nº 10.411, de 30 de junho de 2020, o qual regulamenta a análise de impacto regulatório, a saber:

“Art. 4º A AIR poderá ser dispensada, desde que haja decisão fundamentada do órgão ou da entidade competente, nas hipóteses de:

I - urgência;

II - ato normativo destinado a disciplinar direitos ou obrigações definidos em norma hierarquicamente superior que não permita, técnica ou juridicamente, diferentes alternativas regulatórias;

III - ato normativo considerado de baixo impacto;

IV - ato normativo que vise à atualização ou à revogação de normas consideradas obsoletas, sem alteração de mérito;

.....”

8. Análise jurídica da Procuradoria Federal Especializada (PFE) junto ao ITI

PARECER n. 00006/2024/PROFE/PFE-ITI/PGF/AGU

DESPACHO DE APROVAÇÃO n. 00004/2024/PROFE/PFE-ITI/PGF/AGU

PARECER n. 00024/2024/PROFE/PFE-ITI/PGF/AGU

9. Alterações propostas

Minuta de resolução: Resolucao2xx5_v12_v13_PSS