INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMACAO

NOTA TÉCNICA Nº 6/2017/CGNP/DAFN

PROCESSO Nº 99990.000309/2017-16

INTERESSADO: CONSELHO DA JUSTICA FEDERAL

1. **ASSUNTO**

1.1. Problema na validação dos certificados digitais ICP-Brasil pelos navegadores Chrome e Firefox, em suas versões mais atuais.

1.2. Em 22/05/2017, o representante da AC JUS, Sr. Paulo Martins Inocêncio, encaminhou correspondência eletrônica (SEI nº 0005090) solicitando posicionamento e orientação do ITI sobre o problema na validação dos certificados digitais ICP-Brasil pelos navegadores Chrome e Firefox, em suas versões mais atuais.

2. **INFORMAÇÕES**

2.1. Nas conexões seguras (SSL/TLS), utiliza-se certificado digital, dentre outras funções, para permitir a validação dos nomes dos domínios ou endereço IP pelos aplicativos navegadores de internet.

2.2. Desta forma, navegadores tais como o Chrome da Google, verificam se esse certificado digital foi emitido para o nome de domínio ou IP que se tentou acessar, possibilitando mais segurança para o usuário.

2.3. De fato, desde 1997 havia duas formas de validar um nome de domínio, seja por meio do atributo "*Common Name*" no campo de identificação do titular ou por meio do uso da extensão de identificação de nome alternativo do titular (*Subject Alternative Name-SAN*).

2.4. Em 2000, na publicação da RFC2818 pela IETF, o uso de validação do nome de domínio pelo atributo "*Common Name*" já estava descontinuado devido a ambiguidade e desestruturação desse atributo, ao contrário da extensão *SAN* que permite a estruturação com o uso dos tipos *dNSName* ou *IPAddress* para identificação de domínio.

2.5. A RFC2818 define que se uma extensão *SAN* do tipo *dNSName* estiver presente, esta deverá ser utilizada como identidade, caso contrário, o "*Common Nam*e" do campo "*Subject*" deverá ser utilizado como identidade no processo de validação.

2.6. A RFC2818 também reconhece o uso do "*Common Nam*e" como uma prática comum, porém, estabelece que essa forma está descontinuada e as ACs deveriam se encorajar para utilizar o *dNSName.*

2.7. Ainda que a RFC2818 tenha descontinuado o uso do "*Common Name*", na ausência de qualquer extensão *SAN*, os navegadores admitiam a validação do certificado digital com uso do "*Common Name*".

2.8. A partir da versão 58 do Google Chrome, esse navegador passou a implementar mudanças para reforçar a segurança nas transações eletrônicas, dentre as quais, a remoção do suporte de validação do nome de domínio pelo "*Common Nam*e", conforme orienta a RFC2818. Há indicações, porém, ainda não confirmada, de que o mesmo esteja ocorrendo com a versão mais recente do Mozilla Firefox.

2.9. Quando um certificado digital para SSL/TLS não implementa a extensão *dNSName*, o navegador Chrome em sua versão atual não consegue validar o nome de domínio, gerando uma tela de alerta de site não seguro (SEI nº 0005094), destacando em vermelho e demandando uma confirmação para acesso ao site declarado inseguro.

2.10. A maioria das AC no âmbito da ICP-Brasil não praticam o uso do *dNSName* na extensão *SAN* em seus certificados SSL/TLS, ocasionando falsos alertas de sites inseguros, quando do uso do referido navegador.

2.11. Muitos usuários desses navegadores ao receber a tela de alerta se assustam com a mensagem e deixam de acessar o serviço desejado.

2.12. A insegurança e o desconhecimento de alternativa dificultam a decisão do usuário levando-o à frustração do serviço desejado.

2.13. As normas da ICP-Brasil não restringem o uso do tipo *dNSName*, ou seja, as AC da ICP-Brasil podem implementar a extensão *SAN* do tipo *dNSName* nos certificados SSL/TLS que emitem. Para tanto, requer, antes da emissão de certificados digitais com a referida extensão, a aprovação, pelo ITI, e a publicação em seu repositório da alteração de suas Políticas de Certificado conforme dispostos no documento DOC-ICP-03, alínea "b" do item 3.1, em relação a alteração da PC, e documento DOC-ICP-04, item 7.1.2.6, em relação a admissibilidade de outros campos na extensão *SAN*.

3. **ANÁLISE**

3.1. A RFC2818 é muito clara em orientar as AC a implementarem o uso do *dNSName* para certificados digitais SSL/TLS.

3.2. Devido a existência de aplicações anteriores à RFC2818, admitia-se a validação com uso do "*Common Name*", tornando uma prática comum que vinha perdurando por quase duas décadas.

3.3. Da parte regulatória, não há necessidade de alteração visto que as

normas da ICP-Brasil admitem a implementação do tipo *dNSName* na extensão *SAN*, conforme disposto no documento DOC-ICP-04, item 7.1.2.6.

4. DOCUMENTOS RELACIONADOS

4.1. Correspondência eletrônica (e-mail) da AC JUS enviada pelo Sr. Paulo Martins Inocêncio, assunto: Subject Alternative Name (SEI nº 0005090).

4.2. Tela de alerta de site não seguro (SEI nº 0005094).

5. CONCLUSÃO

5.1. Embora não prescinda de imediata mudança normativa para solução do problema relatado de validação dos certificados digitais ICP-Brasil pelos navegadores Chrome e Firefox, em suas versões mais atuais, sugere-se a submissão do assunto ao Comitê Gestor da ICP-Brasil para regulamentação da obrigatoriedade do campo *Subject Alternative Name* (*SAN*) com o tipo *dNSName*, nos certificados SSL/TLS, em conformidade com a RFC2818.

5.2. Enquanto isso, entende-se que o ITI deva orientar, por meio desse documento, as AC da ICP-Brasil a implementar a extensão *Subject Alternative Name* (*SAN*) com o tipo *dNSName* para identificar nomes de domínio em certificados SSL/TLS e minimizar os problemas de validação relatado pela AC JUS.

5.3. Para tanto, conforme disposto no DOC-ICP-03, item 3.1, alínea "b", há necessidade de submissão ao ITI das novas Políticas de Certificado (PC) pelas AC, para aprovação de mudanças pela implementação da extensão *Subject Alternative Name* (*SAN*) com o tipo *dNSName* que identifiquem nomes de domínios nos certificados SSL/TLS.

Documento assinado eletronicamente por **Wilson Roberto Hirata**, **Coordenador Geral de Normalização e Pesquisa**, em 31/05/2017, às 19:43, conforme horário oficial de Brasília, com o emprego de certificado digital emitido no âmbito da ICP-Brasil, com fundamento no art. 6º, caput, do Decreto nº 8.539, de 8 de outubro de 2015.
Nº de Série do Certificado: 8444201429846164718

A autenticidade deste documento pode ser conferida no site http://[servidor_php]/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0006048** e o código CRC **593C3334**.
