PRESIDÊNCIA DA REPÚBLICA
CASA CIVIL
INFRAESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA
COMITÊ GESTOR

ATA DA REUNIÃO ORDINÁRIA DO COMITÊ GESTOR DA ICP-BRASIL, EM 29 DE ABRIL DE 2014

Aos vinte e nove dias do mês de abril do ano de 2014, nas dependências da sala de reuniões do Instituto Nacional de Tecnologia da Informação – ITI, situado no endereço SCN Qd. 02 Bl. E, na cidade de Brasília/DF, com horário de início previsto para às 09h30, porém, iniciada às 10h30 quando completo o quorum mínimo exigido para deliberações, reuniram-se os membros, Titulares e Suplentes, do Comitê Gestor da ICP-Brasil – CG ICP-Brasil, servidores do Instituto Nacional de Tecnologia da Informação – ITI, representantes por procuração e ouvintes para participar da Reunião ordinária do Comitê Gestor da ICP-Brasil. Estavam presentes: Renato da Silveira Martini (Secretário Executivo do CG ICP-Brasil), Maurício Augusto Coelho (Diretor da DINFRA/ITI – Diretoria de Infraestrutura de Chaves Públicas do ITI), Pedro Paulo Lemos Machado (Diretor da DAFN/ITI – Diretoria de Auditoria, Fiscalização e Normalização do ITI), André Pinto Garcia (Procurador Chefe da Procuradoria Especializada do ITI), Adriana Fetter (Chefe de Gabinete do ITI), Edmar da Silva Araújo (Chefe de Gabinete, substituto do ITI), Fernando Nascimento Barbosa (Titular do Ministério da Fazenda – MF), José Ney de Oliveira Lima (Suplente do Ministério do Planejamento, Orçamento e Gestão – MPOG), George Marmelstein Lima (Titular da Associação dos Juízes Federais do Brasil), José Antônio Carrijo Barbosa (Titular da COTEC e Representante por procuração do GSI/PR-Gabinete de Segurança Institucional), Felipe Sereno (Representante por procuração do Ministério Ciência Tecnologia e Inovação MCTI), Manuel Dantas Matos (Representante por procuração da Camara-e.net), Wander Blanco (Titular da COTEC e Representante por procuração da FEBRABAN – Federação Brasileira de Bancos), Eduardo de Magalhães Lacerda (Assessor Especial do Diretor Presidente do ITI), Ruy César Ramos Filho (Assessor da Diretoria de Infraestrutura de Chaves Públicas do ITI), Pedro Pinheiro Cardoso (Coordenador-Geral da Auditoria e Fiscalização do ITI), Wilson Roberto Hirata (Coordenador-Geral de Normalização e Pesquisa do ITI), André Machado Caricatti (Coordenador-Geral de Operações, do ITI), José Rodrigues Gonçalves Júnior (Coordenador-Geral de Segurança da Informação do ITI), Anderson Nascimento (Ouvinte da Universidade de Brasília – UNB), Maurício Balassiano (Ouvinte pela Camara-e.net), Robson Machado Ouvinte pela Camara-e.net), Fernando

Guimarães Teixeira (Ouvinte da AVIXY Tecnologia), Diogo L. Pinto (Ouvinte da AVIXY Tecnologia), Luiz Cláudio F. Lima (Ouvinte da Caixa Econômica Federal), Sergio Fuchs (Titular da COTEC pelo Ministério da Fazenda), Rodrigo França (Ouvinte pela Receita Federal do Brasil), Carlos Campana (Ouvinte pela VALID), Vinícius Sousa (Ouvinte da Soluti), Michel Medeiro (Ouvinte da Soluti), Angela Maia (Ouvinte pela Soluti),
Pedro Mota (Ouvinte pelo SERPRO), conforme lista de presença.

Dr. Renato abre a reunião pedindo desculpas pelo atraso, justificando o mesmo devido à necessidade de se aguardar a composição mínima de quórum. Apresenta a pauta e propõe alteração da ordem de discussão da mesma. Pergunta aos conselheiros se gostariam de inserir novos temas, não havendo manifestações por parte destes. Segue a reunião para o primeiro item de pauta: 1. Proposta de ajuste de redação no DOC-ICP-04 para compatibilização com aplicações em sistemas ANDROID; Hirata explica que a proposta de alteração objetiva corrigir a redação do DOC-ICP-04 para evitar erro de interpretação. Explica ainda, que o entendimento correto é de que a obrigatoriedade e criticalidade somente deve ser aplicada em certificados para equipamentos de carimbo do tempo (T3 e T4). Para os demais certificados de usuário final, a ICP-Brasil não define a extensão como obrigatória, cabendo às Autoridades Certificadoras a especificação em suas PCs (Políticas de certificado), em conformidade com os regulamentos da ICP-Brasil. Dr. Renato abre a votação. Manuel Matos vota pela aprovação e solicita ajustes de redação à resolução. Registra o voto da Câmara Brasileira de Comércio Eletrônico, com sugestões técnicas a seguir: Isoladamente o texto da alínea e) está escrito corretamente. O que ocorre é que a colocação desta alínea no item 7.1.2.2. que afirma: “A ICP-Brasil define como obrigatórias as seguintes extensões” provoca interpretações equivocadas sobre o uso da extensão *Extended Key Usage.* Como tal extensão só se aplica aos equipamentos de ACT, para que não haja falha de interpretação, recomendamos: 1) Retirar a alínea e) do item 7.1.2.2; 2) Renumerar a alínea f) para e); 3) Criar o subitem 7.1.2.7 com o seguinte teor: Nos certificados de equipamentos de carimbo do tempo de ACT credenciada na ICP-Brasil é obrigatória a utilização da seguinte extensão; 4) Transferir integralmente e sem alterações o texto anteriormente numerado como alínea e) no item 7.1.2.2 para o novo item 7.1.2.7; 5) Feitas essas alterações, o novo item teria a seguinte redação: 7.1.2.7 - Nos certificados de equipamentos de carimbo do tempo de ACT credenciada na ICP-Brasil é obrigatória a utilização da seguinte extensão: *a) "Extended Key Usage", crítica:* deve conter somente o sub-campo *KeyPurposeID* contendo o valor *id-kp-timeStamping* com OID 1.3.6.1.5.5.7.3.8 . Este OID não deve ser empregado em qualquer outro tipo de certificado. Wander da FEBRABAN, concorda com os ajustes propostos pelo conselheiro Manuel Matos. Nenhum outro membro se manifestou sobre os

reajustes. 2. Segundo item da pauta: Hirata, explica a motivação que é a existência de órgãos emissores de RG cuja sigla excede o atual tamanho máximo de 6 (seis) posições. Consulta realizada junto a entidade que atua no serviço de validação de documentos de identificação (BRSCAN) não identificou órgãos emissores com sigla superior à 10 (dez) posições. Assim, recomenda-se máximo de 10 posições , visto que o item 7.1.2.4 do DOC-ICP-04 já orienta a utilização apenas das posições necessárias, da esquerda para a direita, desprezando as posições excedentes ao tamanho máximo. Aberto para votação, Wander Blanco, pede prazo para colocar em ação os campos, de 6 meses – propondo que se estabeleça uma data a partir de quando a alteração passaria a ter efeito, como a partir de 30/10/2014, tendo em vista que os bancos e outras aplicações precisam de tempo para realizar as adequações. Manuel Matos concorda com proposta da FEBRABAN. Manuel Matos manifesta com relação ao ajuste na extensão *Subject Alternative Name*, considera-se que: a) Em consonância com a sugestão apresentada pela FEBRABAN e com a preocupação de que haja prazo suficiente para que as aplicações do mercado sejam adaptadas, vota para que o prazo mínimo da ocorrência de emissão de certificados com a ampliação do tamanho do referido campo seja de 180 dias. b) Adicionalmente, sugere-se que o ITI avalie a possibilidade de estabelecer a prática de emitir comunicados técnicos regulares, sempre que alguma alteração normativa possa gerar impacto sobre a utilização dos certificados digitais pelo mercado. Sugere ainda que os comunicados sejam divulgados no sitio do ITI em área permanente que poderá ser consultada pelo mercado a qualquer tempo. Votou-se pela aprovação dos dois primeiros itens da pauta, com os ajustes apresentados, sendo que a alteração para *Android* terá efeito imediato e para *Other Name* terá validade a partir de 30/10/2014. Concordância de todos conselheiros.

3. Proposta para regulamentação de PSS para ACTs: Hirata explica que esta proposta de alteração objetiva definir parâmetros para a qualificação econômico-financeira com base nos valores exigidos para as solicitações de credenciamento de ACT. Tais parâmetros não estavam estipulados anteriormente. Aberto debate para votação: Manuel Matos, vota pela aprovação da inclusão do valor para Patrimônio Líquido mínimo de 500 mil reais para PSS de ACT. Concordância de todos os conselheiros.

4.Temas provenientes do Grupo de Combate às Fraudes: Renato explica o papel e a atuação do GT de combate à fraudes.

4.1. Centralização da verificação no ambiente da AC: Dr. Renato relata o consenso contrário à proposta ocorrido na COTEC, onde também estiveram presentes a Ancert e a AARB, tendo esta última enviado uma correspondência ao CG ICP-Brasil, ontem a tarde, firmando sua posição contrária. Maurício relata que houve consenso, unânime, pela rejeição da proposta. Mesmo a proposta alternativa de segregar fisicamente as etapas de verificcação e validação nas ARs também

foi integralmente rejeitada. O entendimento geral é de que a centralização da verificação em AC ou a segregação física das atividades na AR não estão proibidas pelas normas da ICP-Brasil, sendo permitido a quem quiser adotá-las, porém, não devem ser obrigatórias. Manuel Matos fala que uma imposição seria uma interferência no modelo de negócio, portanto deve ser facultativa, vota pela rejeição. Dr. Renato pergunta se pode encaminhar pela rejeição. O Comitê Gestor vota por unanimidade pela rejeição, não havendo outras manifestações.

4.2. Envio e consulta dos documentos na base de dados da ICP-Brasil. Dr. Renato pede que Lacerda faça uma apresentação, como fez na COTEC, para demonstrar as ações que se tem feito há 2 anos para combater as fraudes, como a adoção do uso de ferramenta de SW, e elogia a ação dos agentes de registro que tem sido relevante no combate. Foi informado sobre acordo com a Caixa Econômica Federal de modo que quando houver a suspeita de fraude no FGTS, a Caixa irá enviar as informações ao ITI para que se possa identificar o dossiê documental referente ao certificado usado e avaliar se houve ou não a fraude. A proposta apresentada para deliberação é mais um passo no sentido de apoiar a atividade de identificação realizada pelos agentes de registro. Consiste na montagem pelo ITI de uma base de dados das imagens dos documentos utilizados nas emissões de certificados e disponibilização de consulta a esta base pelas ARs (via sistemas das ACs) para comparação com o documento apresentado em processo novos. Dr. Renato relembra que a AC Raiz contava com o projeto RIC para resolver a questão de identificação civil no Brasil, porém, enquanto este não se concretiza, a ICP-Brasil precisa buscar suas soluções, quiçá, constituindo uma base própria. Destaca que o TSE acaba de licitar um sistema AFIS, medida de enorme importância, pois, pode resultar em possível cooperação com o TSE para consulta a essa base biométrica pela ICP-Brasil. Quanto à COTEC, Dr. Maurício relata que não houve consenso. O tema foi polêmico, com manifestações de apoio, mas condicionadas à realização de provas de conceito, e também com argumentos variados contra a proposta como custos, questões de segurança, questionamentos sobre a efetividade da base. Outras sugestões alternativas à proposta foram feitas como envio de e-mail verificador e aproveitamento da base hoje já existente no ITI por conta do envio de informações de emissões de certificados pelas ACs. Estas outras propostas foram registradas e serão avaliadas pelo GT de combate a fraudes. Pedro Cardoso destacou que em todos os casos de fraude apuradas, o fraudador tirou um certificado de pessoas que já tinham um certificado legal, por isso a nossa proposição. Manuel Matos elogia a iniciativa, diz que é boa e completa a argumentação dizendo que talvez fosse melhor adotarmos passos intermediários a antes deste. Se o ITI já tem uma base de todos os certificados emitidos, porque não a disponibiliza para consulta pelas ACs? Lacerda responde que a base de dados biográficos dos certificados não seria efetiva, porque o que se quer apurar agora não são os dados biográficos, que neste tipo de fraude são verdadeiros. É preciso

checar a foto do documento. Seria o único meio de identificar alguma fraude no documento apresentado à AR. Carrijo, representante do GSI/PR, vota pela rejeição. Wander, FEBRABAN, se preocupa com o potencial uso indevido da base, com a possibilidade de quadrilhas infiltradas em nossas ARs usar essa base, preocupação com o nível de segurança, várias considerações sobre a base e suas especificações e testes feitos pela Caixa. Coloca que não quer trazer só problemas e sim soluções alternativas. Cita que os bancos usam critérios para abrir contas, como perguntas específicas durante uma pequena entrevista para verificar as informações pessoais. A ideia do uso de e-mail para a ICP-Brasil verificar se é mesmo a pessoa correta. Proposta de trabalhar com outros ministérios para validação de dados. A questão de disponibilidade teria que ser avaliada. A viabilidade de importação de fotos na base do TSE, tendo em vista o tamanho do arquivo. Utilizar a assinatura digital para emitir os certificados. Foram algumas observações realizadas pelo Sr. Wander. Dr. Renato pede licença para fazer comentários sobre a fala do Wander, colocando que foi riquíssima. Papel do agente de registro: emitir o certificado, acesso a base, comprometimento jurídico, a infraestrutura, o ITI toma conta de duas altamente complexas, concorda com o tema de custo para as ARs, a questão de fraudes do FGTS, a impressão que se tem é que a ICP-Brasil tem um sistema robusto entre outros sistemas, a questão do e-mail para o grande público acha que seria ineficiente, passa a palavra ao Dr. Pedro Paulo e José Ney, depois pede ao Lacerda para demonstrar na prática como é o dia a dia. Dr. Pedro Paulo fala que na COTEC levantou dois aspectos: o seguro não está cobrindo o valor assegurado hoje com as fraudes e o gasto com segurança dever ser visto como investimento. José Ney: é oportuno discutir o tema e o sistema de certificação digital, pois o mesmo é evolutivo, sugere um acordo de cooperação com o TSE na convergência de intenções, encaminhar nossa demanda e termos um projeto cooperativo, e no momento opta pela rejeição da proposta. Lacerda explica que não é ainda uma base biométrica é uma base documental. Trazer uma base biométrica para a ICP-Brasil é fundamental. Discussão acerca da especificação de resolução mínima para digitalização dos documentos opõe entendimentos. Lacerda destaca que há necessidade de melhor a resolução. Cita que algumas digitalizações enviadas para o Comunica Fraude não são adequadas para a identificação do fraudador. O que se quer é um padrão mínimo de resolução para que se possa identificar o fraudador. Destaca que não há dúvida na segurança aplicada à base de dados e ao acesso a ela. O agente de registro entrará na base apenas para consulta, via sistema da AC, identificado pelo seu certificado digital, em processo de emissão de certificado, e não apenas para mera consulta. O agente não terá como modificar ou acessar nenhum dado. De fato, a quantidade de fraudes são mínimas, mas temos convicção na eficiência do processo no combate a estes casos. A experiência anterior, com tudo que o CG ICP-Brasil já aprovou, mostrou sua efetividade. Não temos hoje garantia do envio para um e-mail do próprio cidadão,

muitas pessoas usam um e-mail de outra. Dr. Renato fala que a intenção é discutir o melhor caminho. Ainda que a proposta seja de Instrução Normativa e não Resolução, o ITI trouxe o assunto para deliberação do CG ICP-Brasil. Manuel Matos: vota pela rejeição da proposta e propõe a sequência de consulta à base do ITI. Wander: não contesta a capacidade da robustez da base da ICP-Brasil, porém as duas estruturas são *offline*, qual o custo/benefício do uso da base, a avaliação deve ser um pouco mais criteriosa, rejeita a proposta por não ter uma prova de conceito. Dr. Renato: está pacificado que não há consenso. Fernando do Ministério da Fazenda coloca que é necessário uma prova de conceito e viabilidade tendo em vista os arrazoados colocados aqui, é um assunto importante que não deve ser descartado. Carrijo: o projeto tem que seguir duas premissas, sugiro montar um grupo de trabalho. Dr. Renato fala em seguir a sugestão do Carrijo de montar um grupo para discutir e evoluir no tema. Encaminhamento: criação de um GT para aprofundar o tema, detalhar e avaliar tudo o que foi posto.

5. Proposta de regulamentação de processo para a autorização de uso de novos dispositivos de *hardware* criptográfico ainda não contemplados por MCTs e, portanto, excluídos do processo regular de homologação (INMETRO e/ou LEA); Dr. Renato fala que o tema é pacificado na COTEC. Passa a palavra para o Dr. Maurício que explica que a homologação de novos dispositivos de *hardwares* criptográficos deverá seguir s sistemática atual. Assim, pede a retirada do item de pauta. A ideia é editar uma Instrução Normativa onde se relacionará os novos tipos de hardwares criptográficos com os requisitos de segurança dos MCT hoje já editados, uma vez que o core de segurança é praticamente sempre o mesmo. Não há preocupações com interoperabilidade nestes hws (microSD card, SIM Card + PKI, outros). Destacou que trata-se de demanda forte do mercado para uso seguro de certificados digitais ICP-Brasil em dispositivos móveis e esta medida viabilizará o atendimento de pronto de tal medida. Aplicações hoje usam certificados do tipo A1, mas com a possibilidade de fim destes, há que se viabilizar o uso dos certificados A3 nesses dispositivos. A homologação destes é obrigatória segundo os normativos da ICP-Brasil. Manuel Matos pergunta o prazo. Maurício coloca que será imediato. Proposta de retirada de pauta da proposta original e regulamentação por Instrução Normativa na forma explanada aprovada por todos conselheiros.

6. Proposta de fim da possibilidade de renovação sem identificação presencial para certificados de pessoas jurídicas, tema trazido pela Camara-e.net. Dr. Maurício passa a palavra para o representante da Camara-e.net. Manuel Matos solicita a não deliberação do tema e retirada de pauta. Carrijo concorda. José Ney concorda com a retirada, mas faz uma colocação que nos sistemas de pregões eletrônicos há maciça presença dos pequenos empresários, para verificar qual o impacto disso neste contexto para o pequeno empresário. Fernando ratifica a posição do MPOG, para que haja uma análise do impacto na sociedade. Manuel Matos coloca que depois de um encontro com o Ministro

Afif reconsiderou a posição, para atender os anseios de milhões de empresas, é um projeto mais amplo e somos sensíveis na Camara-e.net. Wander fala que a pessoa jurídica é a vítima preferida nas fraudes. O PJ A1 é um problema nas fraudes, temos que aprofundar esse assunto. Dr. Renato retira de pauta e coloca que o tema do certificado A1 estará em breve na pauta das próximas reuniões pelos problemas que estão sendo colocados.

7. Proposta de regulamentação para a criação de processo simplificado de autorização de novas Instalações Técnicas. Dr. André fala que é um tema trazido inicialmente pela Camara-e.net. A ideia de simplificar o processo é boa tendo em vista a homogenização, mas temos que manter o respeito à cadeia hierárquica da ICP-Brasil. Manuel Matos apoia integralmente o que foi apresentado pelo ITI e parabeniza o trabalho. Proposta aprovada pelo CG ICP-Brasil.

8. Dar ciência do Relatório de Auditoria da AC Raiz. Dr. Maurício relata que todos os membros titulares e suplentes do CG ICP-Brasil receberam o relatório por e-mail. Dr. Renato informa que o relatório é confidencial. Como a reunião está sendo retransmitida ao vivo pela Internet e gravada para posterior disponibilização no canal YouTube do ITI, sugere discutir algum aspecto do relatório, caso queiram, depois da sessão. Manuel Matos apresenta voto da Camara-e.net é pela aprovação do relatório.

9. Informes Gerais: 9.1 Criação de Grupo de Trabalho para redigir o documento de regulamentação do PAdES como padrão de assinatura da ICP-Brasil (DOC-ICP-15.xx): Hirata relata que o GT está criado e com agenda de trabalho elaborada, porém, que ainda é possível a adesão de novos interessados. 9.2. Certforum – 27 e 28 de maio de 2014 - Dr. Renato convida todos os membros do CG ICP-Brasil, neste ano antecipado pelo calendário eleitoral.

Então, deu por encerrada a reunião, agradecendo a presença de todos.

RENATO DA SILVEIRA MARTINI
Secretário Executivo do CG ICP-Brasil
Instituto Nacional de Tecnologia da Informação