



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

ATA DA REUNIÃO EXTRAORDINÁRIA
DO COMITÊ GESTOR DA ICP-Brasil, EM
25 DE AGOSTO DE 2015.

Aos vinte e cinco dias do mês de agosto do ano de 2015, 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 às 14h, 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 e alguns ouvintes para participar da Reunião extraordinária do Comitê Gestor da ICP-Brasil. Estavam presentes: Renato da Silveira Martini (Secretário-Executivo do CG ICP-Brasil), Fernando Nascimento Barbosa (Titular do Ministério da Fazenda – MF), Manuel Matos (Titular da Câmara Brasileira de Comércio Eletrônico – Câmara-e.Net), Ricardo Felipe Custódio (Titular da Sociedade Brasileira de Computação – SBC), Júlio César Rogério Cosentino (Titular da Associação Nacional de Certificação Digital – ANCD), Nivaldo Cleto (Titular da Associação das Autoridades de Registro do Brasil – AARB), José Ney (Suplente do Ministério do Planejamento, Orçamento e Gestão – MPOG), Nubian Mendonça Amorim (Suplente do Ministério do Desenvolvimento, Indústria e Comércio Exterior – MDIC), Marcus Vinícius Amorim Ferreira Guimarães (Suplente do Ministério da Ciência, Tecnologia e Inovação – MCTI), Marcus Vinícius Antunes Liberato (Suplente do Ministério da Justiça – MJ), Marconi dos Reis Bezerra (Suplente do GSI/PR-Gabinete de Segurança Institucional), Rodrigo Timm Wepster (Suplente da Confederação Nacional do Comércio de Bens, Serviços e Turismo - CNC), Antônio Sérgio Borba Cangiano (Suplente da Associação Nacional de Certificação Digital – ANCD), Flávio A. Amorim (Convidado do Conselho Nacional de Justiça – CNJ), Maurício Augusto Coelho (Diretor da DINFRA/ITI – Diretoria de Infraestrutura de Chaves Públicas do ITI), Pedro Pinheiro Cardoso (Diretor da DAFN/ITI, substituto – Diretoria de Auditoria, Fiscalização e Normalização do ITI), André Pinto Garcia (Procurador-Chefe da Procuradoria Especializada do ITI), Eduardo de Magalhães de Lacerda Filho (Assessor Especial do Diretor Presidente do ITI), Ruy César Ramos Filho (Assessor do Diretor Presidente do ITI), Edmar da Silva Araújo (Assessoria de Comunicação do ITI), Alexandre Menezes Ribeiro (Coordenador-Geral, Substituto da Auditoria e Fiscalização do ITI), Wilson

Roberto Hirata (Coordenador-Geral de Normalização e Pesquisa do ITI), José Rodrigues Gonçalves Júnior (Coordenador-Geral de Segurança da Informação do ITI), André Machado Caricatti (Coordenador-Geral de Operações do ITI), Eduardo Jordão (Convidado da ADOBE), João Paulo Foini (Ouvinte da Imprensa Oficial), Saulo Marques (Ouvinte da Imprensa Oficial), Vinícius Rogério (Ouvinte da FEBRABAN), Márcio Viggiani (Ouvinte da SCOPUS), Luiz Zacanella Júnior (Ouvinte da SAFEWEB), Stael Rodrigues Viana (Ouvinte da SAFEWEB), Ângela Maia (Ouvinte da SAFEWEB), Paulo Roque (Ouvinte da AARB), Adriana Narciso (Ouvinte da ANCD), Allan Rocha Coelho (Ouvinte da FENACON CD), Elder Schroder (Ouvinte da FENACON CD), Jean Martins (Ouvinte da UFSC), Vinicius Sousa (Ouvinte da Soluti), Gilberto Netto (Ouvinte do SERPRO), conforme lista de presença. Dr. Renato iniciou a reunião dando as boas vindas e prosseguiu com as apresentações dos membros do ITI e do CGICP-Brasil. Ao término, Dr. Renato falou sobre a Comissão Técnica Executiva - COTEC, solicitando aos Conselheiros do Comitê que enviassem o mais breve a indicação de seus representantes na COTEC, ressaltando que a COTEC não delibera, que é apenas uma forma de discutir, analisar e buscar consenso dos termos técnicos que são demandados pelo Comitê Gestor. Passou então a palavra ao conselheiro Manuel Matos, da Câmara-e.Net, como membro mais antigo do Comitê, para as boas vindas aos novos Conselheiros. Dr. Renato deu sequência com a pauta abaixo:

PAUTA DELIBERATIVA:

1. Aprovação de resoluções *ad referendum* que autorizam a emissão do certificado raiz v4 e aprovam alteração da DPC da AC Raiz para contemplá-lo; Dr. Renato falou da emissão do novo passaporte brasileiro, e que há época de sua implementação foi publicada a resolução *ad referendum*, tendo em vista que, não havia saído as nomeações de todos os Conselheiros do CG ICP-Brasil e, portanto, não havia quorum para deliberações. Passou a palavra para o Dr. Maurício que fez um resumo acerca da necessidade de publicação da referida resolução, tema este, do novo passaporte eletrônico brasileiro, que vem sendo tratado desde 2013 com AC MRE – Autoridade Certificadora do Ministério das Relações Exteriores, para efeito de validação do passaporte brasileiro internacionalmente. O ITI apresenta a Resolução 104 para aprovação *ad referendum*, tendo em vista as dificuldades expostas. Dr. Renato enfocou o esforço do Serpro para que a AC MRE tivesse êxito. Dr. Renato passa a palavra para os conselheiros; Manuel Matos se manifestou favorável, mas pediu para registrar em ata sobre a forma, solicitou a edição da nova resolução para convalidar a resolução 104; Nivaldo

Cleto, manifestou a aprovação da AARB pela aprovação da resolução 104; Dr. André Garcia manifestou-se perguntando se a previsão de aprovação *ad referendum* deverá constar no regimento interno, para poder modificá-lo; Manuel Matos se manifestou contrário a mudança regimental; Nivaldo Cleto está de acordo com a Câmara-e.Net, José Ney ressalta a preocupação com o impacto nas aplicações. Dr. Maurício informou que não há impacto porque essa raiz atende exclusivamente ao passaporte. Aprovado por unanimidade a proposta de nova resolução para convalidação da 104.

2. Autorização para realização de auditorias anuais da AC Raiz por empresa de auditoria independente para os próximos 5 anos (2015 inclusive); Informar sobre necessidade de auditoria da ICP/Brasil incluir requisitos WEBTRUST, para emitir certificados SSL e *Code Sign* (para atender exigências da Microsoft, Mozilla e demais); Dr. Maurício sintetizou o item de pauta, falou do art. 4º da Medida Provisória 2.200 de 24/08/2001, competência deste Comitê, a confiabilidade de um sistema de PKI é baseada na confiabilidade de sua cadeia. Auditorias anuais compatíveis com *webtrust*, proposta de uma resolução que autoriza a AC Raiz a contratar uma auditoria independente para os próximos 5 anos. A empresa vencedora do certame licitatório foi a *Ernest Young*, e a partir da anuência deste Comitê será feita a contratação da mesma. O Acordo com a Adobe para inserção das raízes ICP-Brasil será assinado no próximo CertForum. José Ney fez um aparte e falou das questões dos *mobiles* e a interação com as operadoras de telefonia, Dr. Renato respondeu que a questão do *mobile* é essencial, o ITI já esteve na Anatel e hoje esta questão se torna fundamental para um retorno; outra questão é o *Mozilla*, Dr. Maurício respondeu que já temos 5 anos de discussão com o *Mozilla*, eles recusam a colocar o certificado raiz da ICP-Brasil, temos uma proposta a ser colocada aqui hoje. José Ney falou dos dois grandes projetos no MPOG hoje, o Processo Eletrônico de Informações – PEN e o Sistema Eletrônico de Informações – SEI. Prof. Custódio apresentou uma alternativa, o *trusted service list*(TSL), todos os países europeus têm e o Brasil poderia adotar aqui também esse modelo e o ITI poderia ser o precursor. Dr. Renato falou que pode-se estudar e encaminhar a COTEC esse assunto. Dr. Maurício falou também que é uma proposta a ser avaliada. O Conselheiro Júlio Cosentino colocou que com essas duas ações praticamente se fecha os 100%, toda a parte de telefonia estará incluída. José Ney ressaltou que precisa ter uma certa atenção com esse tipo de proposta. Aprovada a resolução que autoriza a realização de auditorias anuais da AC Raiz por unanimidade.

3. Aprovação de nova versão do DOC-ICP-15 Padrão de Assinatura Digital, com a inclusão do PAdES; Hirata apresentou o tema com um breve histórico: o trabalho foi concluído no início desse ano e em maio foi realizada uma consulta pública e agora estamos submetendo os resultados ao Comitê. Paralelamente estamos desenvolvendo com a UnB um *plug-in para validação do padrão PAdES da ICP-Brasil pelos leitores PDF, Adobe Acrobat Reader inclusive*. Prof. Custódio falou o que se quer na ICP-Brasil é que o pdf possa ser assinado digitalmente, os *mobiles* não vão reconhecer essa assinatura, porque o ISO ainda não reconhece o PAdES, propôs que se espere um tempo, pois estamos pela primeira vez a frente do mundo, vamos aguardar 1 ano para ver o que acontece na Europa. Vamos apoiar o *plug-in* que o ITI contratou. Talvez possamos publicar esse trabalho para sinalizar o mercado. Dr. Renato pediu que fosse explicado o *plug-in* para os presentes. Pedro Cardoso passa a explicar o trabalho que será desenvolvido entre o ITI e a UnB. O *plug-in* acoplado aos leitores reconhecerá a assinatura digital e validará essa assinatura dentro do padrão da ICP-Brasil. Eduardo da *Adobe* falou que entende a preocupação do professor Custódio, mas manifestou apoio à proposta de aprovação já do padrão PAdES ICP-Brasil. Salientou que foi um trabalho benfeito e revisado exaustivamente. Opinou que não teremos avanço no padrão ISO na Europa em um ano, e sugeriu dar continuidade ao trabalho que foi feito nesse período, pois é um padrão 100% aderente a ISO no momento. Nivaldo acrescentou que, se já existe um sistema e a *Adobe* nos diz para colocar no ar, vamos colocar em prática, pois já estamos assinando digitalmente; Manuel Matos manifestou-se bastante semelhante ao Nivaldo e à *Adobe*, favorável pela aprovação nesse comitê do PAdES. Lembrou que o CADES e o XAdES também sofreram aprimoramentos, portanto sugeriu que possamos fazer a aprovação do padrão; Júlio Cosentino está favorável também; Prof. Custódio esclareceu que o PAdES é para preservar a assinatura a longo prazo, já que estamos querendo adotar um padrão brasileiro eu gostaria de ter um SW *compliance* ICP-Brasil, se a maioria quiser apostar nesse pioneirismo temos que ter ciência desse pioneirismo. Eduardo da *Adobe* falou como integrante do grupo de estudo, o *plug-in* fará exatamente isso, a aderência da assinatura. Sugestão para criar um grupo de trabalho permanente na COTEC de acompanhamento, revisão e atualização desses padrões. Câmara-e.Net manifestou voto pela aprovação do PAdES. Os demais acompanham esse voto. José Ney corroborou a criação do grupo de estudos na COTEC, ficando o item 4 aprovado, portanto.

4. Proposta de criação de grupo de trabalho no âmbito da COTEC para revisar Padrão de Assinatura Digital CADES e XAdES; - aprovada no item anterior com a inclusão do PadES também.

5. Proposta de regulamentação para Despersonalização da Pessoa Jurídica nos processos de credenciamento de entidades junto à ICP-Brasil; Dr. André Garcia apresentou o tema, Dr. Renato abriu a discussão para os membros do Comitê. Nivaldo Cleto agradeceu a explicação do procurador-chefe e expressou indignação com o fato de uma entidade ser descredenciada e logo em seguida se credenciar novamente com outro nome. Apoiar a ideia de se achar uma maneira de alcançar as pessoas físicas PFs responsáveis por entidades descredenciadas também, e as ARs que também migram para outras ACs; Júlio Cosentino sugeriu que os antecedentes criminais poderiam ser exigidos na ICP-Brasil, tratando assim de um ponto específico. Dr. André Garcia fez os esclarecimentos solicitados. Nivaldo opinou que para credenciamento no sistema de certificação digital a entidade candidata não pode ter restrição de natureza alguma. Pedro Cardoso explicou que a norma diz que deve-se dizer o motivo do descredenciamento, quando a AC notifica o ITI de graves ilegalidades cometidas pela entidade a ela vinculada. José Ney perguntou se não podemos ter a análise da receita no credenciamento. Dr. André Garcia falou que entende a colocação e vê problema para operacionalizar essa proposta, porque já pedimos no credenciamento todas as certidões negativas. Dr. Maurício acrescentou que nosso objetivo é pontual. No âmbito da ICP-Brasil, se uma entidade foi descredenciada como punição por irregularidades cometidas e não por solicitação, por irregularidades frisou, passa a sujeitar essa PJ e os seus PFs, não voltar mais a ICP-Brasil. Nivaldo, à decisão de descredenciamento cabe uma defesa, como funciona? Dr. André Garcia explicou o fluxo do processo, como este funciona. Votos unânimes pela aprovação da proposta.

6. Proposta de fim da “renovação online não presencial” de certificados PJ. Avaliar se proposta alcançaria também os certificados de pessoa física; Dr. André Garcia explicou que os dados sensíveis das PFs são menos mutáveis que os das PJs. Nivaldo falou que existe uma mudança permanente nas PJs, como contador ele acompanha direto isso na Associação Comercial, vota pela aprovação. Júlio Cosentino falou que apenas um dos associados da ANCD votou negativamente. Que a ANCD é a favor, e queria registrar isso, que são favoráveis. Prof. Custódio falou que facilita para as empresas a renovação *online*, a questão presencial é fazer a conexão entre a pessoa e a chave privada, se houve alguma

outra alteração, isso pode ser encaminhado via internet. Isso pode ser uma complicação para as empresas. Manuel Matos falou que foi ótima a colocação do Professor Custódio, mas a ICP-Brasil nasceu sem renovação, as empresas inicialmente se sentiam mais seguras indo presencialmente. José Ney falou: estamos defendendo o fim do PJ A1, estou preocupado com a pequena e média empresa. Dr. Maurício ressaltou: queremos avaliar a destinação do A1, veremos mais adiante. Existe a preocupação sobre os custos, mas a principal questão é a segurança. O Conselheiro Rodrigo Wepster acrescentou que é do interesse das empresas que não haja aumento de custos, no entanto a questão da segurança é válida, mas questiona se não há outra saída para a questão de segurança. Manuel Matos falou que as observações são todas pertinentes, vivemos numa sociedade que aprendeu a cobrar de seus governantes, tenho acompanhado a luta do ITI para mitigar a questão da segurança e acho que devemos analisar sob a ótica da confiabilidade da ICP-Brasil, que nasceu na confiança, é o momento que a ICP-Brasil tem de dar uma resposta efetiva à tentativa de fraude. Professor Custódio falou que talvez haja uma solução intermediária, a empresa enviar os documentos para a AR e se houver algum problema que se faça necessária a presença dessa pessoa assim a AR a chamaria. Rodrigo falou de duas questões – ampliação de prazo vai na contramão, se esse é o fórum adequado para debater. Júlio Cosentino colocou que a questão de custo é desprezível, em torno de 10% diluído em um ano, Nivaldo falou da preocupação, é o momento de se mostrar que a questão da segurança está sendo levada em consideração. Professor Custódio ressaltou que os atributos do certificado podem se alterar com o tempo, portanto teria que ser revogado. Dr. André Garcia falou que esta revogação já está prevista. O conselheiro Fernando Nascimento pede para poder analisar e deliberar com mais segurança, ter acesso aos dados que dão subsídios a discussão. Dr. Renato esclarece que a COTEC existe exatamente para isso, dar auxílio aos membros do Comitê. Manuel Matos fala da preocupação e citou a matéria passada no Jornal Nacional, onde o repórter colocou o seu espanto com a facilidade de emissão de um certificado que corroborou uma transação na ordem de 11 milhões no IBAMA. Dr. Renato fez a proposta de encaminhamento. Câmara-e.Net votou favoravelmente e pede para que conste em ata que se estenda a mesma proposta para certificado de PF até adoção da biometria. Nivaldo acompanha o voto. Rodrigo colocou o estudo e impacto dos custos. Aprovada a proposta de fim da “renovação online” para certificados PJ..

7. Proposta de estabelecimento de prazo de validade determinado para as procurações públicas - Dr. André Garcia fez uma explanação sobre a proposta; Julio Cosentino aprovou

o pleito; José Ney também aprovou; Rodrigo da CNC, concorda com tudo menos com o prazo, exíguo. Dr. André Garcia informou que os trinta dias para apresentar a procuração não é exíguo; Rodrigo propôs 90 dias; Nivaldo vota com o Rodrigo pelos 90 dias; Dr. André falou que 90 dias é razoável. Item aprovado com o prazo de 90 dias.

8. Proposta de regulamentação do Sistema de Identificação Biométrica da ICP-Brasil. Proposta de implantação da coleta das impressões digitais com brevidade; Eduardo Lacerda apresentou duas resoluções: a primeira alterando o DOC-ICP-05, que consiste na implantação da coleta das biometrias e a segunda alterando o DOC-ICP-05, é dá outras providências, que consiste na implantação da coleta das biometrias e instaura o sistema biométrico da ICP-Brasil. Acrescenta no DOC-ICP-03 o credenciamento de nova entidade na ICP-Brasil, o Prestador de Serviço Biométrico – PSBio, ao DOC-ICP-08 o processo de auditoria e o DOC-ICP-09 o processo de fiscalização dessa mesma entidade. Dr. Renato abriu o debate: o conselheiro Fernando parabenizou o ITI pela iniciativa e sugeriu que ao se encaminhar para a COTEC seja feita uma análise jurídica a luz do processo de identificação civil e o decreto de dados seguros e perguntou se a base de dados não deveria ser mantida pelo próprio ITI. O conselheiro José Ney falou da discussão no MPOG, como também da norma complementar do GSI do uso de biometria, falou do cuidado ao tratar o assunto na COTEC e sugeriu fazer um piloto na administração pública federal, que seria um bom *case*, paralelamente o segmento empresarial seguiria andando. Dr. Renato falou em fazer essa abordagem jurídica na COTEC. Professor Custódio falou que na Europa na maior parte dos países isso é impensável, lá fora a coleta de biometria só é feita para criminoso. O Conselheiro Manuel Matos falou do Projeto de Lei – PL 12 que disciplina a coleta de biometria. O conselheiro Júlio Cosentino falou de uma visão simplista e entende que a biometria seria uma lista positiva. Dr. Renato complementou que a lista de fraudadores, a lista negativa, de julho do ano passado a julho desse ano, foram emitidos cerca de 2 milhões de certificados e desses 262 eram fraudulentos, o que é significativamente positivo, porém um certificado falso na operação da ICP-Brasil é devastador. Dr. Maurício sintetizou que é preciso ter uma unicidade do usuário da ICP-Brasil, essa base distribuída terá no ITI um *backup*, o ITI não emite certificado. Lacerda reforçou que a prioridade é a privacidade da informação. Pedro Cardoso falou da preocupação que até o final do ano teremos 1 fraude a cada 10 mil certificados, o estrago disso no sistema ICP-Brasil é enorme, ou fazemos isso ou o nosso sistema se tornará um sistema comum, falou do caso com o Ibama, quadrilhas atuando agora na ICP-Brasil, ressaltou que o debate é preciso, mas num prazo

exequível para enfrentar a questão da fraude, por isso a necessidade de deliberação. Dr. Renato falou que não podemos ficar na zona de conforto, temos de avançar para novas possibilidades e tecnologias. Encaminhamento: para o envio do material ser discutido na COTEC, de forma imediata; coleta da face e biometria digital para ganhar tempo – Fernando, não se sentiu confortável para deliberar dessa forma, votou por levar os dois assuntos para a COTEC, José Ney votou com o Fernando; Nivaldo falou se a proposta for levar para a COTEC não tem objeção; Júlio Cosentino entendeu que até se formar uma base se levará de 3 a 4 anos, então primeiro é melhor ter uma coleta mandatória, no prazo de 120 dias, prazo exequível para as ACs se ajustarem. Prof. Custódio, propôs levar os 2 assuntos para a COTEC. Rodrigo falou do interesse da CNC em participar da discussão dos 2 assuntos. Dr. Renato Martini informou que o tema será encaminhado a COTEC.

9. Informes Gerais: Dr. Renato sobre o CertForum, as prováveis datas das próximas reuniões do CG ICP-Brasil.

9.1. CertForum – 23 e 24 de setembro de 2015 - CNTC

9.2. - Reuniões mensais, sempre na última terça-feira do mês:
29/09/2015, 27/10/2015 e 24/11/2015

Passou a palavra para o Dr. Maurício que falou dos temas propostos para as próximas reuniões do Comitê

1. Proposta de regulamentação de certificado tipo “mobile”;
2. Proposta de redução do escopo de aplicação do certificado A1 e extinção do certificado A2;
3. Revisão da regulamentação dos certificados de sigilo (tipo “S”);
4. Proposta de alteração do DOC-ICP-10, extinguindo a etapa de homologação pelo ITI de *hardwares* certificados pelo INMETRO;
5. Avaliar a continuidade ou o fim das homologações de *software*;
6. Proposta de alteração do prazo para revogação de certificado de AC de 1º nível pela AC Raiz (DOC-ICP-01, item 4.4.3.3). Definir prazo máximo para situações críticas somente;
7. Proposta de regulamentação de prazo diferenciado para LCRs referentes a certificados

- da AC Raiz revogados (DOC-ICP-01, item 4.4.9);
8. Proposta de exclusão do campo AIA da LCR;
 9. Proposta de obrigatoriedade do uso de OCSP;
 10. Proposta de fim do 3º ponto de distribuição de LCRs na AC Raiz;
 11. Estudos com vistas à adoção de novos algoritmos criptográficos de curvas elípticas e de novos resumos criptográficos (*hashes*);
 12. Proposta de mudança da âncora de tempo para a EAT ICP-Brasil;
 13. Proposta de tornar obrigatória a inserção no programa da Fundação Mozilla dos certificados das ACs que emitem certificados SSL;
 14. Propostas com vistas a robustecer as regras e requisitos para credenciamento, manutenção do credenciamento e descredenciamento de entidades junto à ICP-Brasil, que versarão sobre:

- a) rever requisitos para ACs de 1º e 2º níveis e ARs;
- b) regulamentar objetivamente não-conformidades e correspondentes penalidades na ICP-Brasil;
- c) propor quarentena nos casos de mudança de ACs;
- d) rever critérios para descredenciamento de ACs e ARs;
- e) rever credenciamento simplificado de ARs;
- f) rever acordos operacionais de ARs;
- g) implementar uso obrigatório de dossiês eletrônicos;
- h) rever regulamentação da medida cautelar e instâncias recursais da ICP-Brasil;

Então, Dr. Renato Martini 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