



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

ATA DA REUNIÃO ORDINÁRIA DO
COMITÊ GESTOR DA ICP-BRASIL, EM
30 DE MARÇO DE 2012..

Aos trinta dias do mês de março de 2012, nas dependências 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 14h30 e horário de término às 18h, 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 ordinária do Comitê Gestor da ICP-Brasil. Estavam presentes: Renato da Silveira Martini (Secretário Executivo do CG ICP-Brasil e Diretor-Presidente do ITI), 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 Federal Especializada do ITI), Fernando Nascimento Barbosa (Titular do Ministério da Fazenda – MF), Delfino Natal de Souza (Titular do Ministério do Planejamento, Orçamento e Gestão – MPOG), Paulo Machado (Titular do Ministério da Justiça), Raphael Mandarino Junior (Titular do GSI/PR – Gabinete de Segurança Institucional), Manuel Dantas Matos (Titular da CAMARA e-NET), Francimara Teixeira Garcia Viotti (Titular da FEBRABAN – Federação Brasileira de Bancos), Natan Schiper (Titular da CNC- Confederação Nacional do Comércio de Bens, Serviços e Turismo), Jacob Batista de Castro Junior (Suplente do Ministério do Planejamento, Orçamento e Gestão – MPOG), Marcelo André Barros (Suplente do Ministério da Ciência e Tecnologia), Pedro Pinheiro Cardoso (Coordenador Geral de Auditoria e Fiscalização), Wilson Roberto Hirata (Coordenador Geral de Normalização e Pesquisa do ITI), Eduardo Magalhães Lacerda Filho (Assessor do Diretor Presidente do ITI), André Machado Caricatti (Coordenador Geral de Operações do ITI), Adriana Fetter (Chefe de Gabinete e Assessora da Secretaria Executiva CG ICP-Brasil), Antonio Sérgio Borba Cangiano (Assessor do Diretor Presidente), Maria Isabel Santos (Assessora Gabinete), Patrícia Landim(Assistente técnica do ITI), Ruy César Ramos Filho (Assessor da Diretoria de Infraestrutura de Chaves Públicas do ITI), Edmar Sousa (Representante da Assessoria de Comunicação do ITI), Wander Blanco Nunes (Titular da COTEC da FEBRABAN), Patricia Leite (Ouvinte da Serasa), Edna Santos (Ouvinte da Serasa), Gilberto de Oliveira Neto (Suplente da COTEC do Ministério da Fazenda - MF), Sérgio Roberto Fuchs da Silva (Titular da COTEC do Ministério da Fazenda -MF), Robson Machado (Ouvinte da

CAMARAE-NET), Alessandra Paiva (Assistente Parlamentar CAMARA e-NET) e Adriano Frare (Ouvinte da Imprensa Oficial do Estado de São Paulo – IMESP), conforme lista de presença anexa, para tratar da pauta a seguir: 1 – Padrão de Assinatura Digital; 1.1 – Revisão CADES/XAdES; 1.2 – Grupo para propor a Regulamentação PADES; 2 – Regulamentação do Certificado de Atributo; 3 – Prazo de Validade dos Certificados; 4 – Convalidação de documentos; 5 – Assuntos Diversos; 6 – Informes Gerais. Dr. Renato Martini iniciou a reunião, com quorum para votação deu boas vindas aos membros do comitê gestor, ressaltando que é a instância de deliberação da ICP-Brasil, falando um pouco mais do modelo de governança e então foi à pauta, destacando que dentre os assuntos da pauta o tema mais polêmico é o certificado de atributo. Dr. Renato abordou o tema inicial que é a Revisão dos Padrões de Assinaturas, e a sugestão encaminhada no âmbito da COTEC e da equipe técnica do ITI, é a organização de um Grupo Trabalho para a revisão dos Padrões de Assinatura, que vai analisar e propor a adoção, a alteração ou o descarte de itens pendentes de avaliação provenientes da Oficina realizada na Universidade Federal de Santa Catarina em 2011, com prazo de 30 dias, para conclusão dos trabalhos, e de outro Grupo de Trabalho para propor minuta de regulamentação do Padrão PADES, com prazo de 90 dias para conclusão dos trabalhos. Dr. Renato em ato contínuo pediu que o Hirata, fizesse a apresentação tendo em vista que era um tema pacificado, que não haveria grandes problemas de entendimento. Hirata rememorou o histórico da revisão dos Padrões de Assinatura e falou sobre a melhoria dos Padrões. Que essas propostas foram analisadas pelo ITI, resultando da análise, que das 22(vinte e duas) propostas, foram acatadas 06(seis), 09(nove) foram julgadas improcedentes, e 07(sete) teriam que passar por reavaliação por serem assuntos mais delicados e extremamente técnicos. Hirata acrescentou que os membros da COTEC fizeram a indicação dos representantes de cada grupo e se houvesse mais indicações que fossem encaminhadas via correio eletrônico. Dr. Renato submeteu à votação a criação dos grupos de trabalho e após discussão foram aprovados. Dr. Renato passou ao item da pauta que trata da temporização de Validade dos Certificados, que seria, em parte, o acatamento de uma proposta da FEBRABAN, que discutiu em dezembro do ano passado o tema da expansão da validade dos Certificados das Acs, e também, outra parte, uma proposta que se mostrou bastante polêmica, que é mexer na questão da validade dos certificados de usuários finais, cujo foco era atender à ICAO e ao Passaporte Brasileiro, pois um Certificado Digital da ICP-Brasil, intervém na emissão do Passaporte Brasileiro, e por uma demanda do Padrão ICAO, que padroniza o Passaporte, para atender a padronização do ICAO, o certificado tem que ter maior prazo de validade. não houve polemica na COTEC acerca do tema, mas no decorrer da última semana, surgiram algumas dúvidas. Dr. Renato colocou a proposta de Revisão como encaminhamento, pediu para que Dr. Maurício fizesse a apresentação. Dr. Maurício pontuou que desde que a ICP-Brasil, seja nesse Comitê seja na COTEC, começou as discussões sobre a revisão dos algoritmos e das suítes criptográficas, se aventava a

possibilidade de rever, dada a robustez e fortalecimento dos algoritmos, ampliar os prazos de validade dos certificados. Ainda não havia surgido oportunidade de organizar a discussão, até que na reunião do CG ICP-Brasil do dia 06 de dezembro passado, a FEBRABAN apresentou uma proposta de ampliação no prazo de validade dos certificados de ACs de 1º e 2º nível e a partir disso a proposta foi encaminhada a COTEC, que na reunião do dia 14 de março de 2012, apresentou a questão, tendo sido colocada também a possibilidade de se ampliar o prazo de validade dos certificados de usuários finais, notadamente os certificados do tipo A3 e A4, também os certificados T3 e T4 que vão ser aplicados para as estruturas de Carimbo de Tempo, justamente em cima do critério técnico ou seja suíte criptográfica forte. Uma demanda de mercado por certificados com maior prazo de validade poderia ser atendida, se essa demanda assim se apresentar. A questão técnica era bastante pontual, referente a um problema já apresentado ao ITI na emissão dos passaportes eletrônicos brasileiro. A ICAO tem como norma que o certificado que assina o documento passaporte, tem que ter o mesmo prazo de validade que o passaporte. O passaporte brasileiro tem 5 anos de validade, e hoje não existe um certificado com essa validade. Temos o máximo de 3 anos, e isso causa um problema na hora da validação eletrônica do passaporte, tem hora que ele tenta validar a cadeia, aquele certificado que assinou pode estar vencido, pois o prazo do documento é maior que o próprio certificado que o assinou, isso gerou uma discussão entre o ICAO, a Polícia Federal e a Casa da Moeda, e o ITI entendeu que seria possível hoje pelos HASHES e suítes criptográficas robustas, se ampliar o prazo de validade para contemplar esse case especificamente, e foi elaborada a proposta, apresentada por resolução aos membros. Pedro Cardoso fez uma apresentação detalhando a proposta. A primeira alteração é a proposta de alteração do prazo de validade dos certificados de Autoridades Certificadoras, proposta da FEBRABAN, que já foi discutida e o ITI não vê nenhum problema do ponto de vista técnico. A COTEC, também desta mesma, forma não vê nenhum problema. A situação atual é que esses certificados tem prazo de validade de 10 anos e a proposta é que faça a modificação para que o prazo de validade dos certificados fiquem limitados ao prazo de validade de quem o emitiu. Após apresentação Dr. Maurício fez uma ressalva para o Hirata e Pedro, solicitando a correção do termo utilizado “aprovado pelo comitê gestor “ esclarecendo, o comitê gestor não aprova Hardware. O correto deveria ser “homologado junto à ICP-Brasil”. A ICP-Brasil hoje tem um sistema de homologação de Hardware, então é só promover a correção no texto. Dr. Renato abriu para o debate, Manuel Matos falou que os dois temas são pertinentes: o 1º tema que é o da prorrogação de prazo dos certificados das ACs, já houve uma manifestação da CAMARA e-NET na reunião passada favorável ao tema. Acha que o assunto esta suficientemente maduro para ser debatido, deliberado e aprovado. Quanto ao 2º tema, que envolve aspectos operacionais do dia a dia das ACs, e hoje são inúmeras ACs operando no mercado, concorda que o tema deve ser melhor analisado e debatido

para que se tenha os elementos de convicção suficientes para uma tomada de decisão, principalmente com relação aos certificados do tipo A3 que são os de larga utilização na ICP-Brasil. Com relação ainda a este ponto, as demandas de um certificado de maior prazo, maior segurança, no sentido de utilização do A4, que é um certificado que permitiria neste momento não haver maiores preocupações com relação ao legado já existente, ao estoque já existente na ICP-Brasil de certificados e poderia haver sim um trabalho no sentido de atender as regras da ICAO, as demandas das emissões de passaporte. Manuel Matos consignou que a posição da CAMARA E-NET, com relação a essa segunda proposta, é de que haja uma maior discussão, um maior debate ainda no campo técnico, comercial e operacional principalmente. Dr. Renato relatou que recebeu vários contatos a respeito desses conceitos, que eles acham que isso impactaria na infraestrutura, no planejamento de custos de call center, uma alteração num padrão que na verdade é o padrão dos últimos 10 anos da ICP-BRASIL. Que essas preocupações não foram levantadas no debate da COTEC, mas, após a reunião surgiram as preocupações, em alterar esse padrão que é o padrão atual, que todas as ACs brasileiras, toda a Infraestrutura de Chaves Públicas Brasileira trabalham nos últimos 10. Talvez, a alteração apenas do A4 contemplaria o passaporte e não descontinuará a aplicação, pois, teria o A4 para poder atender. É razoável fazer essa avaliação para não causar nenhum transtorno a essa Infraestrutura. Manuel Matos perguntou como ficaria o encaminhamento por uma questão de ordem, se são duas resoluções diferentes e se o encaminhamento será em separado. Dr. Renato falou que está entendendo que a 1º resolução apresentada (validade de certificados de ACs) está de certa forma validada por todos. Fernando Nascimento lembrou que o Dr. Renato ainda não tinha aberto para votação, que esperou apresentar a outra. Dr. Renato se desculpou e voltou a primeira resolução apresentada por Pedro Cardoso. Dr. Mandarino ressaltou que os assuntos são muito próximos e não tem porque separar as duas resoluções até porque a primeira gera uma certa vantagem para quem está recebendo. Manuel Matos esclarece que ele foi um que se manifestou com as angústias dos seguimentos, assegurando que o que motivou os debates, não foi apenas o prejuízo das operadoras das ACs, existem diversas ACs, que são ACs que pertencem ao serviço público e não à iniciativa privada e assegurou também que não é uma preocupação apenas da indústria da certificação digital e sim também dos usuários que terão certificados com prazo mais longo, e com risco maior. Dr. Renato como proposta de encaminhamento, propôs fazer as alterações das últimas colunas, últimos blocos, que se referem ao A4, S4 e T4, com o compromisso de uma avaliação melhor dos demais casos, para trazer no próximo mês. O ITI vai convocar essa discussão, para amadurecer e enriquecer para que essas dúvidas sejam removidas, superadas para voltar ao debate de forma mais aprofundada. Manuel Matos pediu que Dr. Renato repetisse o encaminhamento, seria a alteração apenas das colunas que dizem respeito ao A4, S4 e T4 que contemplariam o certificado que é a necessidade conjuntural

imediate do passaporte brasileiro. Dr. Renato ressaltou que fica a proposta do compromisso do ITI organizar, de ser o facilitador desse encontro, desse debate, focá-lo na Comissão Técnica que se encontra em outra instancia e por ventura inserir o próprio Comitê Gestor para as questões mais estratégicas. Dr. Mandarino informou que precisava sair porque tinha uma outra reunião, ficando quorum para deliberar. Dr. Renato passou ao item seguinte da pauta que é o grupo que trabalhou sobre fraudes, pediu para Pedro Cardoso fazer a apresentação e após a mesma abriu para debate apresentando duas propostas: primeiro é uma minuta concreta que trata da comunicação de fraudes, que foi submetida e debatida na COTEC sem grandes celeumas, com alguns ajustes de redação, e a outra é a convalidação dos dados biográficos. Os membros concordaram que a primeira minuta é obrigatória, considerando a necessidade de aprimorar as normas operacionais e tecnológicas nos processos de emissão de certificados digitais para minimizar ameaças que possam comprometer a cadeia de confiança da Infraestrutura de Chaves Públicas Brasileira. O Comitê Gestor aprovou a inclusão de um item na minuta de resolução sobre Comunicação de Fraudes. O texto diz que o indício ou fraude comprovada na emissão de certificado por requerente que apresente documento ou informação falsa deverá ser comunicada no dia útil imediatamente subsequente a confirmação do ato. Caberá à AC Raiz, de posse de qualquer notificação de fraude das ACs, propagar todos os detalhes da operação fraudulenta constatada para as ACs de 1º nível. Dr. Maurício ressaltou que a segunda minuta é um ponto que, já existe hoje regulamentado pelo Comitê Gestor que as ACs devem fazer essa validação dos dados biográficos dos documentos apresentados, isso é regulamentado por Instrução Normativa do ITI, e o ITI trouxe ao Comitê por ser uma questão estratégica, que envolve custos, prazos, enfim, alterar-se-ia a Instrução Normativa do ITI, para incluir essa questão da convalidação sistematizada, não implicaria em Resolução, e sim em uma Instrução Normativa do ITI, mas com o conhecimento e aval deste Comitê. A comunicação de fraude independe da Instrução Normativa de Convalidação dos Dados Biográficos. Fernando sugeriu que fosse colocado como “recomendação”, publica-se a Instrução Normativa como uma primeira ação, e o compromisso de esgotar o tema na COTEC. Manuel Matos está de acordo. Francimara falou que ao se recomendar a prática se verá outras possibilidades, julga interessante a recomendação. Manuel Matos falou que em relação ainda a este texto, como uma proteção às ARs, se há a possibilidade de incluir que não havendo o batimento de dados, se a AR tem como recusar a emissão dos certificados. A norma legal prevê a recusa. Alguns cartórios colam os cartazes da ICP-Brasil para que o usuário possa saber. Dr. André falou que a Instrução Normativa previa expressamente a recusa de não havendo o batimento dos dados houvesse a recusa do Agente de Registro, esse é o grande rário da Instrução Normativa. Após discussão a cerca da recusa por parte das ARs, Dr. Maurício sugeriu destacar o assunto para um outro artigo, que assim fugiria da recomendação. Dr. Maurício falou do INMETRO, que pede uma autorização ao Comitê Gestor,

constando em ata, para fazer uma consulta pública do documento dos Requisitos de Avaliação de Conformidade (RAC) para dar prosseguimento á migração do Sistema de Homologação da ICP-Brasil para o Sistema Brasileiro de Avaliação de Conformidade (SBAC), com participação do ITI. Submeteu a autorização para a consulta pública aos membros, o Comitê tomou ciência e aprovou por unanimidade. Delfino precisou sair e deixou o Suplente Sr. Jacob para compor o quorum. Dr. Renato passou ao item da pauta que trata o Certificado de Atributo. Foi um tema bem polêmico na COTEC. Relembrou que a COTEC na governança da ICP-Brasil é uma comissão consultiva que avalia as questões técnicas, o que não a faz menos importante, só que essa comissão só será consultiva se ela tiver uma relação intensa com o membro do Comitê Gestor. A COTEC não pode decidir. Em dezembro do ano passado houve uma decisão quanto ao conceito de certificado de atributo, e sobre isso Dr. Renato chamou a atenção que uma coisa é o conceito do Certificado e a outra coisa é a sua formatação normativa que pode ter várias formas diferentes. Entendeu o ITI em dezembro do ano passado que este comitê tinha decidido pelo conceito de certificado de atributo. A proposta apresentada pelo Dr. Renato foi de primeiro a confirmação do conceito certificado de atributo, segundo preparar a normativa e convocar a COTEC novamente para se debruçar na normativa e estabelecer um tempo para a COTEC preparar essa normativa. Da parte técnica do ITI não temos dúvidas dessa normativa mas a aprovação é do Comitê Gestor e não do ITI. Francimara reforçou que o certificado de atributo ele não é um certificado que assina ele só qualifica. Manuel Matos concorda com a Francimara. Fernando falou que na opinião dele o encaminhamento é de estabelecer uma compatibilidade de prazos dos trabalhos com a COTEC. Manuel Matos falou da questão do prazo de não ser de acordo com mês estabelecido e sim com a quantidade de reuniões, porque as vezes fica para o membro da COTEC responder por algo que não teve condições objetivas de participar. Marcelo falou que tem que haver uma compatibilidade com relação ao tempo e ao esforço que se dá. Dr. Renato pediu ao Ruy uma sugestão de quantidades de reuniões para destrinchar a minuta, Ruy falou que 3 ou 4 reuniões para chegar a uma conclusão Fernando sugeriu que o debate fosse dividido em partes, que uma coisa é discutir o conceito e a outra coisa é discutir o processo, a sugestão é que seja encaminhado a COTEC e tratado em sequencia, gostaria de discutir isso melhor com a COTEC, poderia estabelecer um prazo limite talvez e a COTEC poderia se organizar para fazer esse debate no menor prazo possível. Como proposta de encaminhamento, Dr. Renato, ratificou a criação do Grupo de Trabalho de Regulamentação de Certificados de Atributos que vai aprofundar os estudos técnicos acerca da proposta de regulamentação de certificados de atributos pela ICP-Brasil, o grupo terá como coordenação o Ruy Ramos. Destarte, Dr. Renato deu por encerradas as atividades agradecendo a presença de todos.

RENATO DA SILVEIRA MARTINI
Secretário Executivo do CG ICP-Brasil