PRESIDÊNCIA DA REPÚBLICA
CASA CIVIL
INFRA-ESTRUTURA DE CHAVES PÚBLICAS BRASILEIRA
COMITÊ GESTOR

ATA

ATA DA REUNIÃO DO COMITÊ GESTOR DA ICP-BRASIL, REALIZADA NO DIA 19 DE NOVEMBRO DE 2008.

Aos dezenove dias do mês de novembro de 2008, nas dependências do Instituto Nacional de Tecnologia da Informação - ITI, situado no endereço SCN, Quadra 04, Bloco B, Pétala D, sala 1102, Edifício Centro Empresarial Varig, na cidade de Brasília/DF, às 14h30, reuniram-se os membros do Comitê Gestor da ICP-Brasil conforme lista de presença anexa, para tratar da pauta a seguir: 1 - Apresentação da ATA da reunião do dia 30/10/2008 para discussão e aprovação; 2 - Continuidade da discussão da resolução acerca do Decreto 6.523, de 31 de julho de 2008, que regulamenta a Lei 8078, de 11 de setembro de 1990, para fixar normas gerais sobre o serviço de Atendimento ao Consumidor - SAC; 3 - Apresentação e deliberação acerca da regulamentação de Carimbo de Tempo; 4 - Discussão da proposta da minuta de Regimento Interno para o CG ICP-Brasil e 5 - Apresentação do Resultado do Grupo de Trabalho da COTEC: Revisão dos Algorítimos Criptográficos. 6 - Apresentação do trabalho coordenado pelo ITI sobre regulamentação de Assinatura Digital; 7 - Apresentação do Documento Proposta de regulamentação sobre: AIA; Printable String; Basic Constraints, para deliberação e aprovação. No exercício das atribuições de Coordenador Substituto do Comitê Gestor, Diretor Presidente do ITI e Secretário Executivo do Comitê Gestor da ICP-Brasil Dr. Renato da Silveira Martini, inicia a reunião apresentando os dois pontos centrais da pauta: a aplicação do Decreto 6.523, de 31 de julho de 2008 (SAC) à Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil que foi objeto de debate na reunião passada e Carimbo de Tempo que é considerado um dos maiores compromissos do Comitê Gestor, desde 2002 com a criação de um grupo de trabalho para esse fim. Foi apresentada a servidora Adriana Fetter com atribuição de assessorar os trabalhos da Secretaria Executiva que em ato contínuo, apresentou a ata da reunião realizada nesta Autarquia no dia 30 de outubro do corrente. Dr. Renato informou que

a Ata seria disponibilizada via correio eletrônico para que os membros manifestassem acerca de alguma discordância ou inclusão do teor desta. A Titular da FEBRABAN Francimara Teixera, destacou o Parecer da lavra do Dr. André Garcia Procurador Chefe da Procuradoria Federal Especializada do ITI, sobre a obrigatoriedade da criação do SAC na ICP-Brasil, por se tratar de uma relação de consumo. De forma a consubstanciar esse entendimento foi sugerido a manifestação do Sr. Francisco Rogério Silva Representante da Secretaria de Direito Econômico - SDE. O Suplente da CAMARA e-NET Sr. Helvécio Castello não pode comparecer, mas já havia apresentado alguns contrapontos ao que diz respeito a certificação digital, pois ao seu entendimento não se trata de uma relação de consumo. Dessa forma o Dr. Renato sugeriu ao Titular do CAMARA e-NET, Sr. Manuel Matos, que entrasse em contato com o Sr. Helvécio Castello para que o mesmo enviasse por meio de correio eletrônico seus argumentos a respeito do tema. Em continuidade a discussão Dr. Renato passou a palavra para o Sr. Francisco Representante da Secretaria de Direito Econômico SDE, que inicia suas considerações apresentando alguns critérios norteadores importantes: primeiro o Decreto n° 6.523/2008, que regulamenta o serviço do consumidor, se aplica apenas quando há relação de consumo, consumidor e fornecedor conforme a Lei n° 8078/90; segundo em sendo uma relação de consumo, é aplicável o Decreto para aqueles produtos e serviços que são regulados pelo poder Público Federal, para tanto sugere uma consulta ao DPDC (Departamento de Proteção e Defesa do Consumidor) para compreender um pouco melhor a forma como é provida a relação na Certificação Digital. Para facilitar a deliberação neste momento o DPDC está em caráter prioritário respondendo todas as demandas, Sr. Francisco sugere ao Comitê Gestor a produção de Nota Técnica, provocando esta análise. Para que seja bastante célere esta análise é importante o Departamento de Proteção e Defesa do Consumidor(DPDC) receber elementos que permitam compreender esta relação disto depende esta manifestação. A Procuradoria Federal Especializada – ITI por meio do Procurador-Chefe Dr. André Garcia apresentou o ponto de vista jurídico e pragmático. Do ponto de vista jurídico tem-se uma firme convicção na qual se aplica a legislação à ICP-Brasil consumidor, fornecedor a demanda por um serviço remunerado, elenca também da função social do contrato uma norma Principiológica trazida pelo novo Código Civil, vislumbrou uma vulnerabilidade do consumidor como destinatário final e uma vulnerabilidade técnica jurídica e fática. Do ponto de vista pragmático, uma vez em que um Comitê Gestor deliberando pela não aplicação do Decreto ao sistema, não teria como frear o ímpeto dos Procons Estaduais ou seja, eles seriam perfeitamente livres para aplicar multas, pois sobre o entendimento deles o Decreto não estaria sendo cumprido, então viraria uma questão judicial e poderia gerar uma demanda judicial de cada AC (Autoridade Certificadora) em cada Estado da Federação haja vista que não é uma questão clara, já que os órgãos públicos acolhem as notas técnicas exarada pelo DPDC como caráter diretivo e não vinculativo. Neste prisma, Dr. Renato destaca a argumentação do Dr. André Garcia, pois

independente da resposta do DPDC o Comitê tem que se posicionar mesmo que estes se manifestem da não obrigatoriedade, os Procons podem entender de forma diferente e as AC's serem penalizadas. Dando seqüência Dr. André Garcia leu a Minuta, após leitura, Dr. Renato chama a atenção ao tema, sobre qual tipo de AC o Decreto incidirá. Em seguida Dr. Manoel Matos sugeriu que seja retirado o nº 0800 dos cartões, pois ao vincular o número do telefone do SAC no cartão torna-se em desuso um estoque de mais de dois milhões de cartões emitidos pelas AC's, o que causa prejuízos aos cofres públicos, e sugere que o 0800 do SAC seja informado no termo de titularidade. Definiu-se como encaminhamento a formalização de consulta à SDE, por meio de ofício. Retomando a palavra o Dr. Renato Martini fez uma síntese do andamento sobre a Regulamentação do Carimbo de Tempo, um modelo técnico ancorado na confiança do tempo do observatório nacional, entregando a AC raiz a capacidade de auditoria do tempo e a feitura desse serviço no país. A Coordenadora-Geral de Normalização e Pesquisas, Viviane Bertol, apresenta as Resoluções de n° 50 a n° 61 sobre o tema e o Projeto Normalização do Carimbo de Tempo na ICP-Brasil. As Resoluções foram aprovadas por unanimidade pelo Comitê Gestor, tanto o modelo técnico, como o negocial, que inclui os critérios de credenciamento, tarifas e seguro. A posteriori serão publicadas as Resoluções de n° 50 a n° 61 no Diário Oficial da União e no site. O Diretor de Infra-Estrutura do ITI Maurício Coelho reforçou que o modelo técnico já foi aprovado e complementou com DOC ICP 3 informando que existe uma proposta que é modelo semelhante ao que se aplica hoje nas demais entidades AC's (autoridades certificadoras), AR's (autoridades de registro) e ACT's (autoridades de carimbo de tempo), ou seja em tese qualquer pessoa jurídica pode se credenciar com a ICP-Brasil, preenchendo os requisitos em conformidades financeiras, jurídicas e qualificações técnicas. A Coordenadora Viviane Bertol apresentou também os resultados do grupo de trabalho da COTEC, a revisão dos algoritmos criptográficos, pois a segurança da ICP-Brasil depende das soluções criptográficas empregadas. O objetivo desta revisão é propor novos algoritmos para a ICP-Brasil e um plano de migração dos algoritmos atuais para os novos. O CG ICP-Brasil, determinou que esse trabalho deve ser submetido a consulta pública para definir os prazos de aplicação dos novos algoritmos criptográficos. As principais recomendações do grupo de trabalho são: indicar como os padrões devem ser combinados, de forma que o resultado tenha nível de segurança adequado, como exemplo não é recomendável utilizar uma chave RSA com 4096 bits associada com um hash *SHA1*, pois a fraqueza deste compromete a solução como um todo; que a função hash *SHA1* seja abandonada, e adotada a família do *hash SHA2, SHA256, SHA512 ou Whirlpool*, permitindo assim que o mercado comece a se adaptar aos novos padrões. A função hash Whirlpool é o único utilizado pela União Européia e possui princípios de projeto distintos dos da família *SHA*. A coordenadora Viviane Bertol informou ainda, que a migração dos padrões atualmente em uso na ICP-Brasil para novos padrões é um processo crítico e inadiável, para evitar problemas como ,por exemplo, a chave

da AC-Raiz ser considerada insegura de um momento para outro, e para isso recomenda-se um plano de contingência. O Diretor da Dinfra/ITI Maurício Coelho recomendou não levar em consideração só as questões técnicas, mas os aspectos fáticos, com a possibilidade de por em execução o melhor hash, as questões mercadológicas e os princípios não só o da segurança, mas também o da interoperabilidade, e este trabalho deverá ser levado a consulta pública devido ao impacto. Dr. Renato sugere que essa consulta seja inserida no site do ITI. Professor Custódio da Universidade Federal de Santa Catarina UFSC, lembra do hash que é uma preocupação Mundial sugeriu que o CG acompanhasse as atividades do Laboratório de teste *National Institute of Standards and Technology* - NIST (USA) quanto a escolha de um novo padrão de hash que será denominado de SHA-3. Sugere ainda criar um plano de contingência emergencial ICP-Brasil AC raiz. O CG ICP-Brasil aprovou também o Documento da Regulamentação sobre Printable String após deliberação da proposta, apresentada pela coordenadora Viviane Bertol. Dada a exigüidade de tempo Dr. Renato sugeriu passar o item faltante da pauta, Regulamentação de Assinatura Digital, para a próxima reunião convocando os membros do CG ICP-Brasil com data prevista para o dia 09 de dezembro do corrente.

.....
RENATO DA SILVEIRA MARTINI
Coordenador,Substituto do CG da ICP-Brasil