

e-PING

**Padrões de Interoperabilidade de
Governo Eletrônico**

Respostas aos questionamentos encaminhados à Consulta Pública 2007

Brasília, 18 de dezembro de 2007

Sumário

Respostas Relativas à Parte Geral do Documento.....	3
Respostas Relativas ao GT – Interconexão.....	13
Respostas Relativas ao GT – Segurança.....	27
Respostas Relativas ao GT – Meios de Acesso.....	39
Respostas Relativas ao GT – Organização e Intercâmbio de Informações.....	47
Respostas Relativas ao GT – Áreas de Integração para Governo Eletrônico.....	50

Respostas Relativas à Parte Geral do Documento

1) CONTRIBUIÇÃO:

3. Políticas Gerais

Retirar a definição de que padrões proprietários serão aceitos apenas de forma transitória, bem como a preferência a soluções de Software Livre.

Justificativa: No Documento de Referência e-PING v 2.9 é declarada a preferência por padrões abertos em detrimento dos padrões proprietários, bem como a preferência por soluções de Software Livre. Da forma como está redigida, ela antes de tudo é um tanto imprecisa. Aparentemente, essa política trata como disjuntos os padrões abertos e os padrões proprietários, mas existem padrões que são ao mesmo tempo abertos e proprietários. O conceito de "padrão aberto" pode se fundamentar em princípios jurídicos, comerciais ou eminentemente técnicos, e uma definição consensual desse conceito é improvável de se conseguir, pelo menos em um futuro próximo. Supostamente, esse conceito foi evocado dentre as políticas gerais da e-PING para conduzir à construção de certas características técnicas nos padrões a serem adotados. Em vez de sustentar a especificação dos padrões da e-PING em um conceito difuso como o dos "padrões abertos", pode ser mais apropriado explicitar as características técnicas desejadas para que um padrão seja adotado. Quanto à preferência por soluções de Software Livre, ela poderia ser retirada da e-PING, pois está fora de contexto: a e-PING trata da especificação de padrões para interoperabilidade, e definitivamente não trata e não deve tratar da especificação dos aplicativos que irão interagir com base nesses padrões. Qualquer manifestação de preferência ou indução ao uso de aplicativos com quaisquer características específicas contraria o princípio que tem motivado o desenvolvimento dos padrões para interoperabilidade expressos na e-PING. A inclusão da preferência de uso de aplicativos de código livre na especificação do protocolo de interoperabilidade da e-PING suscita uma discussão que está fora do contexto desse protocolo. Qualquer referência a escolha de produto ou solução deve ser tarefa exclusiva da equipe técnica responsável pela especificação da solução e, portanto, item de projeto de implementação e não de política de interoperabilidade.

Responsável: Raimundo Nonato da Costa

Enviada em: 15/11/2007 10:30

RESPOSTA:

Igual à resposta 4.

2) CONTRIBUIÇÃO:

3. Políticas Gerais

Retirar a restrição a adoção de padrões proprietários de forma transitória, bem como a preferência a soluções de Software Livre

Justificativa: No documento de Referência e-PING versão 2.9 é declarada a preferência por padrões abertos, em detrimento dos padrões proprietários, bem como a preferência por soluções de Software Livre. Da forma como está redigida, ela antes de tudo é um tanto imprecisa. Aparentemente, essa política trata como disjuntos os padrões abertos e os padrões proprietários, mas existem padrões que são ao mesmo tempo abertos e proprietários. O conceito de "padrão aberto" pode se fundamentar em princípios jurídicos, comerciais ou eminentemente técnicos, e uma definição consensual desse conceito é improvável de se conseguir, pelo menos em um futuro próximo. Supostamente, esse conceito foi evocado dentre as políticas gerais da e-PING para conduzir à construção de certas características técnicas nos padrões a serem adotados. Em vez de sustentar a especificação dos padrões da e-PING em um conceito difuso como o dos "padrões abertos", pode ser mais apropriado explicitar as características técnicas desejadas para que um padrão seja adotado. Quanto à preferência por soluções de Software Livre, ela poderia ser retirada da e-PING, pois está fora de contexto: a e-PING trata da especificação de padrões para interoperabilidade, e definitivamente não trata e não deve tratar da especificação dos aplicativos que irão interagir com base nesses padrões. Qualquer manifestação de preferência ou indução ao uso de aplicativos com quaisquer características específicas contraria o princípio que tem motivado o desenvolvimento dos padrões para interoperabilidade expressos na Referência e-PING. A inclusão da preferência de uso de aplicativos de código livre na especificação do protocolo de interoperabilidade da e-PING suscita uma discussão que está fora do contexto desse protocolo.

Considerando que o objetivo da e-PING é a interoperabilidade, deveria ser evitada referência a itens de projeto ou estratégias de implementação que resvala nos processos comerciais que eventualmente podem se desenvolver no futuro.

Essa é uma tarefa de responsabilidade do implementador e portanto, deveria ser tratada no seu tempo.

Responsável: Raimundo Nonato da Costa

Enviada em: 15/11/2007 10:40

RESPOSTA:

Igual à resposta 4.

3) CONTRIBUIÇÃO:

"Abrir" as tabelas de padrões classificados nas categorias A/R/T/E/F, incluindo uma ressalva de que outros padrões não mencionados explicitamente poderão ser usados, desde que atendendo às diretrizes da e-PING.

Justificativa: Na seção 5.4.1 Seleção e Homologação de Padrões Tecnológicos, os padrões candidatos a integrar a especificação da e-PING são classificados em cinco categorias. No documento correspondente da e-GIF britânica, observamos que os padrões candidatos são classificados em quatro categorias, que coincidem aproximadamente a quatro das cinco categorias encontrados na Referência e-PING. A análise comparativa das quatro categorias que têm correspondentes no documento da e-GIF britânica permite identificar oportunidades de aperfeiçoamento da Referência e-PING, e é questionável se a quinta categoria deve ser mantida na Referência e-PING.

As categorias que constam tanto na Referência e-PING como na documentação da e-GIF britânica são:

? A ? Adotado: um padrão classificado como Adotado tem poder determinante nos processos de interação entre sistemas. A proposta de solicitar homologação externa à Gestão da e-PING para classificar um padrão como Adotado é uma boa forma de salvaguardar a integridade da especificação da e-PING. Impedir que a classificação como Adotado pudesse advir de forma autônoma da Gestão da e-PING deve ser visto como um mecanismo de proteção da própria equipe gestora, bem como de manutenção de consistência da especificação. A atual redação da Referência e-PING não exige a homologação externa, e nossa opinião é de que a Referência e-PING poderia ser ajustada nesse sentido.

? R ? Recomendado: um padrão classificado como Recomendado pode ser interpretado como um padrão selecionado pela Gestão da e-PING, que ainda não foi homologado por um agente externo. Essa interpretação pressupõe o ajuste da Referência e-PING conforme sugerido acima. Segundo a atual redação da Referência e-PING, não existe diferença clara entre padrões classificados como Adotado ou como Recomendado, e essa imprecisão pode ser fonte de conflitos e dificuldades futuras.

? E ? Em Estudo: um padrão classificado como Em Estudo pode ou não evoluir para uma das classes acima.

? F ? Estudo Futuro: um padrão classificado como Estudo Futuro é um padrão já identificado, mas que ainda não foi colocado em estudo sistemático. Esse padrão pode ou não evoluir para a classe Em Estudo.

A categoria que consta da Referência e-PING, mas não consta da e-GIF britânica, é a categoria T ? Em Transição. Essa categoria de padrões é utilizada para os padrões atualmente em uso, mas que a Gestão da e-PING recomenda deixar de serem utilizados. Nas listas de padrões da Referência e-PING essa categoria é utilizada sem indicação explícita do motivo da classificação (ou seja, de quais políticas técnicas não estariam sendo atendidas pelo padrão classificado como Em Transição). Ademais, as listas de padrões da Referência e-PING são ?fechadas?, ou seja, elas supostamente são

listas completas, contendo todos os padrões relevantes para a especificação da e-PING. Em contraste com isso, a documentação da e-GIF britânica não discrimina padrões atualmente em uso como padrões que devem ter seu uso descontinuado, e apresenta listas de padrões sempre "abertas", ou seja, finalizadas por uma indicação que pode ser interpretada como: "Quaisquer outros padrões podem ser utilizados além dos considerados explicitamente nesse documento, desde que eles atendam às políticas técnicas propostas pela e-GIF".

Essa diferença sutil de redação muda significativamente o caráter, a precisão técnica e o potencial de melhoria de eficácia dos processos de interoperabilidade da Referência e-PING em comparação com a documentação da e-GIF britânica. Enquanto que a especificação britânica é necessariamente inclusiva e favorece a interoperabilidade entre sistemas tanto legados como projetados para interação automática, a especificação da e-PING contendo padrões classificados como Em Transição e listas "fechadas" de padrões cria a possibilidade de discriminação de padrões e aplicações, o que pode levar a restrições de interoperabilidade entre sistemas. Ou seja, a Referência e-PING pode, em decorrência dessa imprecisão em sua especificação, ser mal utilizada e produzir resultados divergentes dos esperados: em vez de favorecer e ampliar a interoperabilidade entre sistemas, limitar essa mesma desejada interoperabilidade.

Responsável: Flavio Soares Correa da Silva

Enviada em: 15/11/2007 17:19

RESPOSTA:

Caro Senhor Flávio,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, informamos que a sua contribuição foi parcialmente aceita.

Esclarecemos que para a utilização do documento de referência da e-PING primeiro deve-se buscar os componentes de seu interesse nas "Especificações Técnicas" dos cinco segmentos. Como a e-PING apenas trata das especificações que forem relevantes para garantir a interconectividade de sistemas, integração de dados, acesso a serviço de governo eletrônico e gerenciamento de conteúdo e como o documento de referência está próximo da terceira versão, pode acontecer que o componente buscado não esteja disponível nas "Especificações Técnicas". Assim, deve-se buscar orientação nas "Políticas Técnicas". Caso as "Políticas Técnicas" também não possuam as orientações necessárias, deve-se consultar as "Políticas e Premissas Gerais" da e-PING. Além disto, todos os órgãos poderão sugerir novos componentes através das consultas públicas, das audiências públicas e da participação dos servidores nos grupos de trabalho.

Com relação à homologação, a regra é que haja a homologação externa à coordenação, já que será realizada por "(...) *uma instituição do governo ou por uma outra instituição com delegação formal para realizar o processo*". Nos casos especiais, a homologação ocorre por proposição do

coordenador do Grupo de Trabalho e aprovação da Coordenação da e-PING, após publicação no sítio da e-PING para que sejam enviadas contribuições pelos órgãos, empresas e sociedade.

A principal diferença entre o padrão “recomendado” e o padrão “adotado” é que apesar de atender à todas as políticas definidas na arquitetura e-PING, o padrão recomendado ainda não passou por um processo de homologação. Lembramos também que os componentes classificados como “adotado” são de uso compulsório pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP).

Com relação aos componentes classificados como “em transição”, esclarecemos que a atual versão do documento de referência da e-PING somente apresenta componentes classificados como “em transição” no segmento “Meios de Acesso”, sendo que, em quase a totalidade dos casos, o motivo principal destes estarem classificados como “em transição” é o não atendimento à política geral de adoção preferencial de padrões abertos. Informamos que em sua versão futura, o documento da e-PING irá explicitar os motivos pelo qual o componente está classificado como “em transição”.

Quanto à utilização de listas fechadas, a e-PING possui as características de não ser exaustiva, ser dinâmica, com versões anuais, e a medida em que surgem novas necessidades estas são tratadas pela arquitetura.

Atenciosamente,
Coordenação da e-PING

4) CONTRIBUIÇÃO:

3. Políticas Gerais

Retirar a limitação imposta ao padrões proprietários como Transitórios, bem como a referência a soluções de Software Livre

Justificativa: No Documento de Referência da e-PING V 2.9 é declarada a preferência por padrões abertos, em detrimento dos padrões proprietários, bem como a preferência por soluções de Software Livre. A adequabilidade de sua inclusão na especificação da arquitetura e-PING merece uma avaliação cuidadosa.

Aparentemente, essa política trata como disjuntos os padrões abertos e os padrões proprietários, mas existem padrões que são ao mesmo tempo abertos e proprietários. O conceito de “padrão aberto” pode se fundamentar em princípios jurídicos, comerciais ou eminentemente técnicos, e uma definição consensual desse conceito é improvável de se conseguir, pelo menos em um futuro próximo. Supostamente, esse conceito foi evocado dentre as políticas gerais na e-PING para conduzir à construção de certas características técnicas nos padrões a serem adotados. Em vez de sustentar a especificação dos padrões da e-PING em um conceito difuso como o dos “padrões abertos”, pode ser mais apropriado explicitar as características técnicas desejadas para que um padrão seja adotado. Quanto à preferência por soluções de Software Livre, ela poderia ser retirada da e-PING, pois está fora de contexto: a e-PING trata da especificação de padrões para

interoperabilidade, e definitivamente não trata e não deve tratar da especificação dos aplicativos que irão interagir com base nesses padrões. Qualquer manifestação de preferência ou indução ao uso de aplicativos com quaisquer características específicas contraria o princípio que tem motivado o desenvolvimento dos padrões para interoperabilidade expressos na e-PING. A inclusão da preferência de uso de aplicativos de código livre na especificação do protocolo de interoperabilidade da e-PING suscita uma discussão que está fora do contexto desse protocolo, e pode induzir à vinculação da Referência e-PING e sua utilização a políticas de adoção de aplicativos para uso interno nos órgãos do governo federal, o que pode implicar em atrasos desnecessários na implantação ampla e efetiva da arquitetura e-PING.

Considerando que o objetivo da e-PING é a interoperabilidade, essa diretriz parece mais adequada. Além do mais, a referência a produtos ou soluções específicas são itens que deveriam estar presentes somente como parte do projeto de implementação, pois já aponta para questões de natureza comercial. Essas preocupações deveriam ser parte somente dos itens que envolvem o processo de desenvolvimento da solução e nunca na política de interoperabilidade. Portanto, tais referências deveriam ser retiradas da e-PING.

Responsável: Raimundo Nonato da Costa

Enviada em: 15/11/2007 17:24

RESPOSTA:

Caro Senhor Raimundo,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Em resposta à sua proposta de retirada da limitação imposta aos padrões proprietários no documento de referência, reiteramos nossa compreensão de que a atual redação, alinhada às políticas gerais de todos os governos que têm trabalhado o tema da interoperabilidade, apresenta-se como aspecto estratégico para a defesa do interesse público. Afinal, os riscos em estabelecer dependência de fornecedor exclusivo em temas tão críticos para a gestão pública e sociedade, quanto aos sistemas de informação, são conhecidos e documentados.

Relevante destacar que os aspectos contidos em seu comentário em relação às dificuldades de estabelecer definição consensual e “perfeita” do que sejam padrões abertos são pertinentes e neste sentido buscaremos aperfeiçoar as referências ao termo em versões futuras.

Quanto à escolha preferencial de soluções em Software Livre, isto ocorre em função das diretrizes, dos objetivos e das ações prioritárias do governo federal no Planejamento Estratégico produzido pelo Comitê Técnico de Implementação de Software Livre.

Lembramos também que a e-PING não faz “(...) qualquer manifestação de preferência ou indução ao uso de aplicativos com quaisquer características específicas (...)” já que a arquitetura e-PING faz referência a padrões e não a produtos ou fabricantes. Desta forma, qualquer produtor ou fabricante

que trabalhe com os componentes indicados no documento de referência da e-PING poderá participar de qualquer processo de compra e contratações do governo federal, Poder Executivo, direcionado para o desenvolvimento de serviços de governo eletrônico e para atualizações de sistemas legados, conforme recomendações da e-PING.

Atenciosamente,
Coordenação da e-PING

5) CONTRIBUIÇÃO:

Enfatizar o interesse em ser inclusivo na especificação da e-PING no que se refere à interoperabilidade.

Justificativa: A interoperabilidade é bem apresentada na Referência e-PING, que na seção 2 (Escopo) a caracteriza como o fundamento para propiciar a conexão (informacional) do governo, tanto no âmbito interno (ou seja, entre órgãos do próprio governo) como no contato com a sociedade brasileira (pessoas físicas e jurídicas usuárias das informações do governo), com outros governos e com a sociedade internacional (pessoas físicas e jurídicas não necessariamente brasileiras usuárias das informações do governo).

O foco da e-PING é enfatizado nessa seção do Documento de Referência, esclarecendo o interesse em especificar exclusivamente padrões para interoperabilidade, conectividade e intercâmbio de dados e serviços.

Naturalmente, como a interoperabilidade é um processo multilateral, também o governo passa a alcançar com esse processo o acesso eficaz a informações provenientes da sociedade brasileira, de outros governos e da sociedade internacional. Esse ponto merece ser enfatizado e considerado na especificação técnica da arquitetura e-PING, uma vez que ele explicita o interesse em ser tão inclusivo quanto possível na interoperabilidade e intercâmbio de serviços e dados. Esse interesse de inclusão conduz, implicitamente, a maximizar também a inclusão de formatos de serviços e dados.

Responsável: Flavio Soares Correa da Silva

Enviada em: 15/11/2007 18:30

RESPOSTA:

Caro Senhor Flávio,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, informamos que houve interpretações diversas entre os integrantes

da Coordenação da e-PING. Desta forma solicitamos à Vossa Senhoria que encaminhe o seu questionamento ao endereço eletrônico da e-PING (eping@planejamento.gov.br) de maneira mais específica, para que possamos respondê-la da melhor forma.

Atenciosamente,
Coordenação da e-PING

6) CONTRIBUIÇÃO:

5. Gestão da e-PING

Proponho que seja incluído um quadro contendo as metas de evolução e realizações planejadas para a e-PING, versão seguinte. É importante compartilhar a visão de futuro e direcionamento dos trabalhos da e-PING, bem como indicar os resultados obtidos. Seria interessante dispor que um quadro com as realizações até a versão corrente, bem como o que está planejado para a versão seguinte. O quadro deveria ter uma coluna com a meta/descrição e outra coluna com o valor/indicador alvo aferido (a ser alcançado).

Justificativa: Oferecer um mecanismo que compartilhe a previsão do que será feito para a próxima versão do documento e das iniciativas de interoperabilidade que o e-GOV.br deseja implementar. A existência de "níveis de situações" das especificações técnicas não atinge o objetivo de visibilidade sobre os próximos passos e compromissos planejados.

Responsável: Paulo Cezar Czarnewski
Enviada em: 16/11/2007 16:44

RESPOSTA:

Caro Senhor Paulo,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, informamos que será implementado no sítio da e-PING um campo informando as metas de cada um dos Grupos de Trabalho para as próximas versões do documento de referência da e-PING.

Atenciosamente,
Coordenação da e-PING

7) CONTRIBUIÇÃO:

5. Gestão da e-PING

Incluir nas atribuições das atividades de Gestão, a possibilidade de analisar projetos de integração de sistemas e interoperabilidade entre serviços de e-gov, objetivando operacionalizar mecanismos de financiamento ou suplementação orçamentária aos órgãos envolvidos na implementação do projeto. A equipe de gestão teria a incumbência de analisar projetos e identificar oportunidades de financiamento para a sua execução. O acompanhamento e fiscalização da execução do projeto seria de responsabilidade dos órgãos de controle (CGU, TCU, etc).

Justificativa: Incluir mecanismos que permitam o fomento as iniciativas de implementação de soluções de interoperabilidade entre sistemas e órgãos da APF, sem que essa iniciativa fique limitada ao montante orçamentário que cada órgão dispõe para cumprir com as suas necessidades cotidianas de TIC.

Responsável: Paulo Cezar Czarnewski

Enviada em: 16/11/2007 16:58

RESPOSTA:

Caro Senhor Paulo,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo à sua proposição, registramos que em uma primeira análise este aspecto transcende o escopo da arquitetura e-PING. Há no entanto alguns elementos iniciais, referentes ao tema, que podem instruir o tratamento atual do assunto, como pode ser observado em um dos pontos de atuação da Coordenação da e-PING: *“Gestão dos processos de contratação dos serviços e de estabelecimento de convênios para realização das atribuições necessárias para consolidação dos padrões, como, por exemplo, avaliação de propostas de projetos de e-gov voltados para a Administração Pública Federal, homologação de padrões e verificação de conformidade;”*. Além disto, como atribuições de caráter administrativo da e-PING, podemos citar: *“Gerenciar a interação com órgãos de fomento nacionais e internacionais, para canalizar recursos, visando atender as necessidades de criação de infra-estrutura da e-PING e promover a pesquisa e desenvolvimento;”* e *“Atuar cooperativamente, como apoio aos órgãos de governo, na realização dos processos necessários para adequação aos padrões e-PING; avaliar a possibilidade de patrocinar programas abrangentes que promovam a utilização intensiva dos padrões propostos.”*. Lembramos também que é dever de cada um dos órgãos que compõem o SISP: *“Alocar e suprir recursos para dar suporte aos seus processos de adequação à e-PING;”*. Sendo esta a síntese do tema até o momento, informamos que poderemos vir a retomar o assunto futuramente.

Atenciosamente,
Coordenação da e-PING

Respostas Relativas ao GT – Interconexão

1) CONTRIBUIÇÃO:

Alterar o item "Segurança de Conteúdo de Mensagem Eletrônica" da seção 6.2 ("Interconexão: Especificações Técnicas"), para "O S/MIME v3 deverá ser utilizado quando for apropriado para segurança de conteúdo de mensagens gerais do governo, a menos que os requisitos de segurança determinem outra forma."

Justificativa: Existe uma inconsistência entre o item "Segurança de Conteúdo de Mensagem Eletrônica" da seção 6.2 ("Interconexão: Especificações Técnicas"), e os itens "Segurança de redes IPv4 para protocolos de aplicação" e "Conteúdo de e-mail" da seção 7.2 ("Segurança: Especificações Técnicas"). O primeiro item recomenda o uso de S/MIME v3.1, enquanto os outros dois recomendam o uso de S/MIME v3. Sugerimos alterar o disposto na seção 6.2 para "S/MIME v3" para manter a consistência com o disposto na seção de segurança.

Responsável: Fernando Antonio Montenegro Cima

Enviada em: 09/11/2007 13:50

RESPOSTA:

Caro Senhor Fernando,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, não é conveniente alterar o item "Segurança de conteúdo de mensagem eletrônica" de S/MIME v3.1 para v3.0. Estaríamos recuando na definição dos componentes, já adotada em versões anteriores do documento. Existe a RFC3851 (<http://rfc.net/rfc3851.html>), relativa ao S/MIME v3.1, que torna obsoleta a RFC2633, relativa ao S/MIME v3, recomendada pelo GT de Segurança.

A questão será remetida ao GT2 para análise da possibilidade de alteração dos componentes de segurança para versão S/MIME v3.1.

Atenciosamente,

Coordenador do GT1 da e-PING

2) CONTRIBUIÇÃO:

No item 6.5 onde estão as especificações de Virtual Private Network (VPN), sugiro acrescentar o uso de protocolos de tunelamento.

Justificativa: Uma VPN é construída sobre uma infraestrutura de rede pública enquanto mantém a privacidade através de procedimentos de segurança e protocolos de tunelamento como por exemplo o L2TP (Layer Two Tunneling Protocol). Através desses protocolos é possível cifrar os dados que serão enviados e decifrar os recebidos, uma vez que esses dados são enviados através de um "túnel" que não pode ser "invadido" por dados que não foram cifrados corretamente. Outro nível de segurança também é possível, não apenas cifrando os dados mas também os endereços de origem e destino.

Responsável: Vinicius dos Santos Livramento

Enviada em: 15/11/2007 12:01

RESPOSTA:

Caro Senhor Vinicius,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, acatamos a sugestão, entretanto sem especificar tipos de protocolo, pois tal assunto é tratado no capítulo de segurança do documento de referência da e-PING.

Atenciosamente,

Coordenador do GT1 da e-PING

3) CONTRIBUIÇÃO:

No item 6.5 onde estão as especificações de Virtual Private Network (VPN), sugiro acrescentar o uso de protocolos de tunelamento.

Justificativa: Uma VPN é construída sobre uma infraestrutura de rede pública enquanto mantém a privacidade através de procedimentos de segurança e protocolos de tunelamento como por exemplo o L2TP (Layer Two Tunneling Protocol). Através desses protocolos é possível cifrar os dados que serão enviados e decifrar os recebidos, uma vez que esses dados são enviados através de um "túnel" que não pode ser "invadido" por dados que não foram cifrados corretamente. Outro nível de segurança também é possível, não apenas cifrando os dados mas também os endereços de origem e

destino.

Responsável: Vinicius dos Santos Livramento

Enviada em: 15/11/2007 12:03

RESPOSTA:

Igual à resposta 2.

4) CONTRIBUIÇÃO:

No item 6.5 onde estão as especificações de Virtual Private Network (VPN), sugiro acrescentar o uso de protocolos de tunelamento.

Justificativa: Uma VPN é construída sobre uma infraestrutura de rede pública enquanto mantém a privacidade através de procedimentos de segurança e protocolos de tunelamento como por exemplo o L2TP (Layer Two Tunneling Protocol). Através desses protocolos é possível cifrar os dados que serão enviados e decifrar os recebidos, uma vez que esses dados são enviados através de um "túnel" que não pode ser "invadido" por dados que não foram cifrados corretamente. Outro nível de segurança também é possível, não apenas cifrando os dados mas também os endereços de origem e destino.

Responsável: Vinicius dos Santos Livramento

Enviada em: 15/11/2007 12:38

RESPOSTA:

Igual à resposta 2.

5) CONTRIBUIÇÃO:

No item 6.3, onde se fala sobre os Web Services, sugiro acrescentar informações sobre as desvantagens de sua utilização.

Justificativa: Naturalmente os Web Services tem algumas desvantagens. A principal delas é o overhead. Transmitir os dados em XML é obviamente menos eficiente do que usar código binário. O que você ganha em portabilidade, você perde em eficiência. Apesar disso, este overhead é geralmente aceitável para a maioria das aplicações, mas você nunca encontrará aplicações críticas em tempo real que usam Web Services.

Responsável: Guilherme Schoepping

Enviada em: 16/11/2007 09:28

RESPOSTA:

Caro Senhor Guilherme,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, sabemos que *Web Services* possui desvantagens, assim como toda tecnologia. As vantagens e desvantagens das tecnologias e dos padrões preconizados pela e-PING são discutidas durante o processo de construção do documento. Quando um padrão ou tecnologia está com a situação de Recomendado pela e-PING é porque já houve um período de discussão e concluiu-se que aquela seria a melhor opção. Assim sendo, entendemos que não cabe elencar todas as vantagens e desvantagens de tecnologias ou padrões no documento da e-PING. Entretanto, queremos ressaltar que estamos elaborando um Guia de orientação para a implementação de *Web Services* e neste guia certamente levaremos em consideração a sua contribuição.

Atenciosamente,

Coordenador do subgrupo: *Web Services*

6) CONTRIBUIÇÃO:

No item 6.6 onde se encontra a descrição de redes P2P, sugiro adicionar uma breve descrição dos problemas de segurança enfrentados por este tipo de rede.

Justificativa: Embora redes P2P possam contribuir para o compartilhamento de recursos e a colaboração em larga escala, em ambientes geograficamente distribuídos, com controle descentralizado e acoplamento fraco, sofre de sérios problemas de segurança.

Ao almejar que redes P2P sejam amplamente adotadas, elas precisam estar protegidas contra a ação de nodos maliciosos. Esses podem fornecer, propositalmente, respostas incorretas a requisições tanto no nível de aplicação quanto no de rede. No primeiro caso, retornando informações não verdadeiras em resposta a uma busca, na tentativa de censurar o acesso a determinados objetos. No segundo, fornecendo informações falsas sobre rotas, visando particionar a rede. Além dessas, atacantes podem realizar outras atividades maliciosas tais como análise de tráfego (inclusive em sistemas que buscam oferecer anonimidade) e censura naqueles que desejam prover alta disponibilidade.

Responsável: Ari Silveira Anselmo Junior

Enviada em: 16/11/2007 12:36

RESPOSTA:

Caro Senhor Ari,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, incorporaremos ao item 6.6. parte de sua sugestão ao texto.

Atenciosamente,

Coordenador do GT1 da e-PING

7) CONTRIBUIÇÃO:

No item 6.3, onde se fala sobre os Web Services, sugiro acrescentar informações sobre as desvantagens de sua utilização.

Justificativa: Naturalmente os Web Services tem algumas desvantagens. A principal delas é o overhead. Transmitir os dados em XML é obviamente menos eficiente do que usar código binário. O que você ganha em portabilidade, você perde em eficiência. Apesar disso, este overhead é geralmente aceitável para a maioria das aplicações, mas você nunca encontrará aplicações críticas em tempo real que usam Web Services.

Responsável: Guilherme Schoepping

Enviada em: 16/11/2007 15:52

RESPOSTA:

Igual à resposta 5.

8) CONTRIBUIÇÃO:

No item: "6.1.1. Os órgãos da APF deverão se interconectar utilizando IPv4 e planejar sua futura migração paraIPv6. Novas contratações e atualizações de redes devem prever suporte à coexistência dos protocolos IPv4 e IPv6 e a produtos que suportem ambos os protocolos." sugiro que o padrão IPv6 seja adotado primariamente ao invés de agendar uma futura migração.

Justificativa: O padrão IPv4 se tornará não mais viável a partir de 2010 devido ao mesmo suportar apenas 4 bilhões de endereços, enquanto o padrão IPv6 suporta até 3.4×10^{38} ; sem contar as vantagens do novo padrão perante ao velho, como a possibilidade do DHCP ser omitido e o suporte para opções de segurança como autenticação, integridade e confidencialidade dos dados entre muitas outras.

O governo americano já determinou que todas as suas agências federais devem suportar o protocolo IPv6 até o ano que vem. Por que não podemos ser tão rápidos quanto eles?

Responsável: Roberto Marinho

Enviada em: 16/11/2007 16:33

RESPOSTA:

Caro Senhor Roberto,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, é importante salientar que a e-PING acompanha as tendências de mercado e o contexto em que o setor público está inserido. Neste sentido, não é possível obrigar uma migração sumária para o IPV6 se esta ainda não é a realidade tecnológica em que os órgãos e entidades usuários da e-PING estão inseridos.

Atenciosamente,

Coordenador do GT1 da e-PING

9) CONTRIBUIÇÃO:

No item 6.4 onde está descrito o uso do email, sugiro a inserção de um texto introdutório sobre a tecnologia.

Justificativa: Mensagem Eletrônica (e-mail) é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação. O termo e-mail é utilizado em sistemas que utilizam a Internet e são baseados no protocolo SMTP.

O envio e recebimento de uma mensagem de e-mail é realizado através de um sistema de correio eletrônico. Um sistema de correio eletrônico é composto de programas de computador que suportam a funcionalidade de Cliente de Correio e de um ou mais servidores de e-mail que, através de um endereço de correio eletrônico, conseguem transferir uma mensagem de um usuário para outro. Estes sistemas utilizam protocolos de Internet que permitem o tráfego de mensagens de um

remetente para um ou mais destinatários que possuem computadores conectados à Internet. O formato na Internet para mensagens de e-mail é definido na RFC 2822 (<http://www.ietf.org/rfc/rfc2822.txt>).

Mensagens de e-mail consistem basicamente de duas seções principais:

*cabeçalho (header) ? é estruturado em campos que contém o remetente, destinatário e outras informações sobre a mensagem.

*corpo (body) ? contém o texto da mensagem.

Responsável: Roque Oliveira Bezerra

Enviada em: 16/11/2007 18:59

RESPOSTA:

Caro Senhor Roque,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, acreditamos não ser necessário um texto introdutório com a abordagem sugerida, pelo conhecimento geral que se tem sobre correio eletrônico.

Atenciosamente,

Coordenador do GT1 da e-PING

10) CONTRIBUIÇÃO:

No item 6.4, referente a Mensagem Eletrônica, sugiro que seja posto o texto introdutório abaixo:

Justificativa: Mensagem Eletrônica (e-mail) é um método que permite compor, enviar e receber mensagens através de sistemas eletrônicos de comunicação. O termo e-mail é utilizado em sistemas que utilizam a Internet e são baseados no protocolo SMTP.

O envio e recebimento de uma mensagem de e-mail é realizado através de um sistema de correio eletrônico. Um sistema de correio eletrônico é composto de programas de computador que suportam a funcionalidade de Cliente de Correio e de um ou mais servidores de e-mail que, através de um endereço de correio eletrônico, conseguem transferir uma mensagem de um usuário para outro. Estes sistemas utilizam protocolos de Internet que permitem o tráfego de mensagens de um remetente para um ou mais destinatários que possuem computadores conectados à Internet. O formato na Internet para mensagens de e-mail é definido na RFC 2822 (<http://www.ietf.org/rfc/rfc2822.txt>).

Mensagens de e-mail consistem basicamente de duas seções principais:

*cabeçalho (header) ? é estruturado em campos que contém o remetente, destinatário e outras informações sobre a mensagem.

*corpo (body) ? contém o texto da mensagem.

Responsável: Roque Oliveira Bezerra

Enviada em: 16/11/2007 19:03

RESPOSTA:

Igual à resposta 9.

11) CONTRIBUIÇÃO:

Na Tabela 1 - Especificações para interoperabilidade, no item Protocolos de Transferencia de Arquivos, a inserção do protocolo SFTP (SSH File Transfer Protocol) para estudos futuros.

Justificativa: Este protocolo de transferencia de arquivos já é adotado como padrao pelo SILC (Secure Internet Live Conferencing) e possui diversas descrições na IEFT para possíveis futuras padronizações.

O seu uso garantiria sigilo das informações transferidas, sigilo este primordial dentro de instituições governamentais e empresas.

Responsável: Luiz Paulo de Farias Junior

Enviada em: 16/11/2007 21:17

RESPOSTA:

Caro Senhor Luiz,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, o GT2 aceitou a sugestão e será colocada na situação EM ESTUDO.

Atenciosamente,

Coordenador do GT1 da e-PING

12) CONTRIBUIÇÃO:

Na Tabela 1 - Especificações para interoperabilidade, no item Protocolos de Transferencia de Arquivos, a inserção do protocolo SFTP (SSH File Transfer Protocol) para estudos futuros.

Justificativa: Este protocolo de transferencia de arquivos já é adotado como padrao pelo SILC(Secure Internet Live Conferencing) e possui diversas descrições na IEFT para possíveis futuras padronizações.

O seu uso garantiria sigilo das informações transferidas, sigilo este primordial dentro de instituições governamentais e empresas.

Responsável: Luiz Paulo de Farias Junior

Enviada em: 16/11/2007 21:19

RESPOSTA:

Igual à resposta 11

13) CONTRIBUIÇÃO:

Na Tabela 1 - Especificações para interoperabilidade, no item Protocolos de Transferencia de Arquivos, a inserção do protocolo SFTP (SSH File Transfer Protocol) para estudos futuros.

Justificativa: Este protocolo de transferencia de arquivos já é adotado como padrao pelo SILC (Secure Internet Live Conferencing) e possui diversas descrições na IEFT para possíveis futuras padronizações.

O seu uso garantiria sigilo das informações transferidas, sigilo este primordial dentro de instituições governamentais e empresas.

Responsável: Luiz Paulo de Farias Junior

Enviada em: 16/11/2007 21:20

RESPOSTA:

Igual à resposta 11

14) CONTRIBUIÇÃO:

Uso de STUN para facilitar transmissão de dados via protocolos Peer-To-Peer através da implementação de do protocolo STUN em servidores públicos e seguros.

Justificativa: O Protocolo STUN, é amplamente utilizado para facilitar a transmissão de voz e dados via UDP quando eles estão atrás de gateways NAT. Como o protocolo depende de um servidor e os disponíveis gratuitamente podem não ser seguros seria interessante que exista no documento menção sobre a implantação da tecnologia, pois seria útil para protocolos como SIP, que não funcionam corretamente quando atrás de um gateway NAT.

O servidor STUN permite que os clientes descubram seu endereço público, o tipo de NAT utilizado, e o lado da porta da Internet associada à NAT com uma porta local específica. Essas informações são usadas para permitir a comunicação UDP entre clientes, e então, estabelecer a conexão. O protocolo STUN é definido pela RFC 3489.

Responsável: Eduardo Felipe Castegnaro

Enviada em: 16/11/2007 21:21

RESPOSTA:

Caro Senhor Eduardo,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, o entendimento do GT1 ainda é no sentido de não se utilizarem aplicações P2P devido aos diversos problemas de segurança que apresentam.

Atenciosamente,

Coordenador do GT1 da e-PING

15) CONTRIBUIÇÃO:

No Ítem Mensageria em Tempo Real da Tabela 1, ítem 6.2 substituir a recomendação do protocolo IMPP pelo mais atual XMPP

Justificativa: O protocolo sugerido, IMPP, foi tornado obsoleto pela ampla aceitação e utilização do mais moderno XMPP. O Protocolo XMPP, definido em RFC 3920 e RFC 3921, é um protocolo extensível para troca de mensagens e presença que, por ser aberto e baseado em XML, pode ser facilmente acoplado a plataformas SOAP via namespaces, podendo assim construir funcionalidades

sobre o protocolo central.

O protocolo IMPP foi originalmente feito para ser transitório e seu desenvolvimento foi cessado em 2003 quando o XMPP foi aceito como padrão.

Sendo assim adotá-lo seria um problema para a interoperabilidade visto que ele não é suportado por nenhum cliente comumente utilizado.

O XMPP possui diversas implementações livres, inclusive clientes desenvolvidos especialmente para a utilização em Browsers, o que é o foco do e-Ping.

Visando segurança qualquer servidor XMPP pode ser isolado da rede pública além disso, fazem parte das especificações XMPP medidas de segurança robustas, usando SASL e TLS.

Sendo assim creio que sua utilização possa facilitar a interoperabilidade de maneira superior ao IMPP.

Responsável: Eduardo Felipe Castegnaro

Enviada em: 16/11/2007 22:01

RESPOSTA:

Caro Senhor Eduardo,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, o GT1 da e-PING resolveu adotar sua sugestão, substituindo a recomendação do protocolo IMPP pelo protocolo XMPP.

Atenciosamente,

Coordenador do GT1 da e-PING

16) CONTRIBUIÇÃO (encaminhada via e-mail):

Transferência de Arquivos

6.1.6. Os protocolos FTP e/ou HTTP devem ser utilizados para transferência de arquivos, observando suas funcionalidades para recuperação de interrupções e segurança, quando necessário. O HTTP deve ser priorizado para transferências de arquivos originários de páginas de sítios da Internet.

Componente: Protocolo de transferência de arquivos:

FTP (RFC 959 e RFC 2228) (com re-inicialização e recuperação)

HTTP (RFC 2616) para transferência de arquivos. (status: R)

6.1.7 Para tráfego de informações que não sejam de divulgação pública deverão ser utilizados obrigatoriamente mecanismos de segurança, tais como a extensão segura do FTP (RFC2228), file transfer em SSH (sFTP) ou cliente específico (confirmar se podemos citar um cliente)

Componente: Protocolos de transferência segura de arquivos:

FTP com extensão segura (RFC 959 e RFC 2228) (com re-inicialização e recuperação) (status:A)

file transfer em SSH (sFTP) (status: R)

cliente/servidor de transferência segura bsdFTPd * (status: R)

* sugestão de solução cliente/servidor baseada em sw livre, onde o servidor roda em Linux e os clientes rodam em diversas plataformas (Windows, Linux, FreeBSD, etc)

Componente: Rede Local Sem Fio (status: R)

IEEE 802.11 b/g, em conformidade com as determinações do Wi-Fi Alliance (<http://www.wi-fi.org>) e com as normas da Anatel (<http://www.anatel.gov.br>), devendo suportar WPA (wi-fi protected access) e IEEE 802.11i (segurança em wi-fi)

Responsável: Odilon de F. Militão

Enviada em: 15/10/2007 19:57

RESPOSTA:

Caro Senhor Odilon,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, o GT2 aceitou parcialmente as sugestões, da seguinte forma: o FTP não será recomendado para transferência segura de arquivos, nem mesmo, com a extensão da RFC 2228; o SSH FTP será incluído na situação EM ESTUDO e quanto ao uso do bsdFTPd, não tem sido prática do GT2 recomendar implementações específicas.

Com relação ao componente Rede Local Sem Fio, a especificação será restringida ao 802.11b/g, sendo os aspectos de segurança tratados no GT2.

Atenciosamente,

Coordenador do GT1 da e-PING

17) CONTRIBUIÇÃO (encaminhada via e-mail):

Bom dia

Gostaria de fazer uma pequena contribuição com algumas idéias sobre os possíveis usos de uma VPN e sobre o algoritmo de criptografia simétrica AES.

O documento em anexo contém um texto básico falando sobre o assunto.

Obrigado

Uma VPN (Virtual Private Network, ou Rede Privada Virtual), pode ser utilizada, além da função de tunelamento sobre uma rede insegura, como uma ferramenta para criar diferentes camadas que sobrepõe uma rede interna por exemplo.

Um exemplo de uso dessa funcionalidade é quando, em um órgão público ou qualquer outro lugar, se quer permitir que uma pessoa que chegue com um notebook e possa ter acesso à rede sem fio provida pelo lugar, mas se deseja esconder desse usuário qualquer máquina, informação, compartilhamento que sejam secretos. Usando uma VPN, pode ser criada uma rede virtual que tenha acesso somente à rede externa e máquinas # permitidas # da rede interna e fazer com que um usuário que tente acessar a rede sem as credenciais necessárias seja direcionado para essa rede.

Essa funcionalidade também pode ser utilizada para isolar grupos diferentes de um mesmo local, setor financeiro do de TI, por exemplo, permitindo que um possa visualizar somente os dados que o outro deseja que ele veja.

Outra funcionalidade que pode ser obtida pela VPN é a maior proteção contra vírus e outras formas de ataque, pelo uso das chamadas SSL/TLS VPNs (VPN sobre o protocolo SSL/TLS, ao invés de IPSec). Esse tipo de VPN pode utilizar uma autenticação baseada em TLS, onde somente as máquinas que possuam uma certa chave definida pelo administrador possam iniciar algum tipo de comunicação com a rede protegida.

As VPNs sobre SSL/TLS também oferecem a grande vantagem da existência de softwares livres de ótima qualidade que permitem o seu uso e configuração. Um bom exemplo é o projeto OpenVPN, que implementa os serviços VPN com base em todas as funcionalidades de criptografia e segurança fornecidas pelo projeto OpenSSL, biblioteca de segurança livre que vem sendo reconhecida como uma das melhores em existência.

Responsável: Rafael Meneguzzo Sartor

Enviada em: 16/11/2007 10:26

RESPOSTA:

Caro Senhor Rafael,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, esclarecemos que documento de referência da e-PING não trata das possibilidades de aplicações e implementações dos protocolos nele descritos.

Atenciosamente,
Coordenador do GT1 da e-PING

Respostas Relativas ao GT – Segurança

01) CONTRIBUIÇÃO:

Alterar o item “Transferência de Arquivos de Forma Segura” da seção 7.2 (“Segurança: Especificações Técnicas”) para “FTPS RFC 4217 (<http://www.ietf.org/rfc/rfc4217.txt>) e HTTPS RFC 2818 (<http://www.ietf.org/rfc/rfc2818.txt>).”

Justificativa: O protocolo FTP (RFCs 959 e 2228) não implementa mecanismos de criptografia das credenciais de usuário e dos dados trafegados, razão pela qual acreditamos que deveriam ser retirados da lista de protocolos recomendados para transferência segura de arquivos. Sugerimos a substituição pelo protocolo FTPS (RFC 4217), que implementa mecanismos de criptografia usando TLS, em conformidade com o padrão recomendado RFC 2246 e compatível com o uso de certificados digitais emitidos no âmbito da ICP-Brasil.

Responsável: Fernando Antonio Montenegro Cima

Enviada em: 09/11/2007 14:07

RESPOSTA:

Caro Senhor Fernando,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, o GT2 aceitou a contribuição parcialmente, pois entendeu que deve-se retirar as referências atuais quanto as RFCs 959 e 2228 e acrescentar a sugestão apresentada na condição de EM ESTUDO, de modo a permitir maiores discussões sobre o Componente.

Atenciosamente,

Coordenador do GT2 da e-PING

2) CONTRIBUIÇÃO:

Alterar o item “LAN sem fio 802.11 g” da seção 7.2 (“Segurança: Especificações Técnicas”) para “O uso da especificação IEEE 802.11i com o padrão 802.11g deve ser incentivado, uma vez que a proteção oferecida pelo padrão WEP (Wired Equivalent Privacy) apresenta vulnerabilidades.”

Justificativa: O padrão IEEE 802.11i, também conhecido como WPA2, provê melhor segurança que o WPA por utilizar CCMP e AES (padrão recomendado e-PING) ao invés de TKIP e RC4. Vale

lembrar que, ao contrário do 802.11i, o WPA nunca chegou a ser padronizado dentro do âmbito do IEEE nem de nenhum outro organismo de standards.

Responsável: Fernando Antonio Montenegro Cima

Enviada em: 09/11/2007 14:17

RESPOSTA:

Caro Senhor Fernando,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, a contribuição será aceita parcialmente, considerando que houve um erro material ao digitar WPA, quando deveria ter sido digitado WPA2, conforme discussões colocadas em Ata. Após revisão o GT2 sugere o uso do padrão 802.11-2007, com o WPA2.

Atenciosamente,

Coordenador do GT2 da e-PING

3) CONTRIBUIÇÃO:

Alterar o item “Informática forense” da seção 7.2 (“Segurança: Especificações Técnicas”) para Guide to Integrating Forensic Techniques into Incident Response NIST - Special Publication 800-86 (<http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>), e alterar a sua categoria para R Recomendado.

Justificativa: O documento não se encontra mais em estado Draft, estando sua versão Final já disponível no endereço listado na contribuição.

Responsável: Fernando Antonio Montenegro Cima

Enviada em: 09/11/2007 14:22

RESPOSTA:

Caro Senhor Fernando,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, o GT2 aceitou a recomendação, pois está coerente com o pensamento do grupo. A idéia de colocar o texto como EM ESTUDO foi no sentido de permitir maiores discussões, mas agora, entende-se que é oportuna a alteração para RECOMENDADO.

Atenciosamente,
Coordenador do GT2 da e-PING

4) CONTRIBUIÇÃO:

Na tabela 3 do item 7.2, na linha sobre a transferência de dados nas redes, sugiro a adição dos hashes SHA-224 e SHA-384, da família SHA-2.

Justificativa: Esses hashes podem ser utilizados para melhorar o desempenho e diminuir a redundância de dados em transferências que não necessitem de um hash grande. Por exemplo: aplicações com muitas trocas de mensagens pequenas.

Responsável: Gustavo Alexssandro Tonini
Enviada em: 11/11/2007 22:27

RESPOSTA:

Caro Senhor Gustavo,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, o GT2 resolve aceitar parcialmente, pois entende que as funções de hash SHA-224 e SHA-384 deve ficar na condição EM ESTUDO, considerando que foram incluídas no Relatório Final do Grupo de Trabalho de Criptografia I, instituído pelo Gabinete de Segurança Institucional da Presidência da República, porém, ainda não se transformaram em norma na Administração Pública Federal.

Atenciosamente,
Coordenador do GT2 da e-PING

5) CONTRIBUIÇÃO:

No item "Segurança", evitar o uso dos hashes da família SHA-1.

Justificativa: Esta família de hashes será inutilizada em breve (recomenda-se usar até 2008) e não seria legal adicionar tecnologias ultrapassadas em um padrão novo.

Responsável: Gustavo Alexssandro Tonini

Enviada em: 11/11/2007 22:40

RESPOSTA:

Caro Senhor Gustavo,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, informa-se que foi aceito, considerando que o algoritmo SHA-1 não foi incluído no Relatório Final, de 09/11/2007, do Grupo de Trabalho de Criptografia I, instituído pelo Gabinete de Segurança Institucional da Presidência da República.

Atenciosamente,

Coordenador do GT2 da e-PING

6) CONTRIBUIÇÃO:

Na tabela 4, onde estão as especificações de Segurança de Correio Eletrônico, sugiro acrescentar uma nova linha tratando do uso de criptografia nas mensagens de e-mail.

Justificativa: A assinatura digital garante a integridade e autenticidade da mensagem, porém não existe a opção de criptografar a mensagem enviada.

Essa funcionalidade deve ser incluída pois algumas mensagens devem ter caracter sigiloso.

Responsável: Arthur Fragnani Medeiros

Enviada em: 14/11/2007 16:20

RESPOSTA:

Caro Senhor Arthur,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, o GT2 entendeu que já está contemplado no Componente

“Conteúdo de Email”, que se encontra na Tabela 4 – Especificações Técnicas para Segurança de Correio Eletrônico.

Atenciosamente,
Coordenador do GT2 da e-PING

7) CONTRIBUIÇÃO:

Na tabela 3 do item 7.2, na linha sobre a transferência de dados nas redes, sugiro a adição dos hashes SHA-224 e SHA-384, da família SHA-2

Justificativa: Os mesmos podem ser utilizados para melhorar o desempenho e diminuir a redundância de dados em transferências que não necessitem de um hash grande. Por exemplo: aplicações com muitas trocas de mensagens pequenas.

Os hashes SHA-224 e SHA-384 são versões simplificadas dos hashes SHA-256 and SHA-512 e por este motivo consomem menos recursos, sendo indicados para uso neste tipo de aplicação. O padrão FIPS 180-2 define:

SHA-224 é idêntico ao SHA-256, exceto:

- * Os valores iniciais das variáveis h0, h1, ..., h7 são diferentes e
- * A saída é construída omitindo h7.

SHA-384 é idêntico ao SHA-512, exceto:

- * Os valores iniciais das variáveis h0, h1, ..., h7 são diferentes e
- * A saída é construída omitindo h6 e h7.

É importante permitir que os desenvolvedores de cada aplicação escolham o hash que melhor se adapta à mesma, devido a grande diversidade de protocolos de comunicação e formatos de transferências que podem ser utilizados pelos mesmos.

Responsável: Gustavo Alexssandro Tonini
Enviada em: 15/11/2007 16:32

RESPOSTA:

Caro Senhor Gustavo,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência

da e-PING.

Relativo ao seu questionamento, o GT2 resolve aceitar parcialmente, pois entende que as funções de hash SHA-224 e SHA-384 deve ficar na condição EM ESTUDO, considerando que foram incluídas no Relatório Final do Grupo de Trabalho de Criptografia I, instituído pelo Gabinete de Segurança Institucional da Presidência da República, porém, ainda não se transformaram em norma na Administração Pública Federal.

Atenciosamente,
Coordenador do GT2 da e-PING

8) CONTRIBUIÇÃO:

Utilizar, além do 3DES e do AES, o algoritmo de ciframento Blowfish na tabela 5 do item 7.2

Justificativa: O Blowfish é um algoritmo de ciframento simétrico altamente difundido e de domínio público. Ele aceita chaves de 32 a 448 bits, o que o torna bastante flexível. É um dos algoritmos de ciframento mais rápidos em uso. Sugiro adicioná-lo como ?recomendado?.

Responsável: João Eduardo Hornburg

Enviada em: 16/11/2007 16:28

RESPOSTA:

Caro Senhor João,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, resolveu-se não aceitar a inclusão do algoritmo Blowfish em razão de ser mais um algoritmo que realizaria a mesma função que o AES. A discussão sobre desempenho de algoritmos precisaria ser estudada e comprovada em laboratório. Faltaria também ao Blowfish uma entidade de caráter público que o mantenha, que é uma premissa utilizada na e-PING.

Atenciosamente,
Coordenador do GT2 da e-PING

9) CONTRIBUIÇÃO:

A contribuição a seguir se refere ao Documento de Referência da e-PING ? Versão 2.9, item 7.2. Segurança: Especificações Técnicas, Tabela 4 ? Especificações Técnicas para Segurança de Correio Eletrônico.

Componente: Assinatura

Justificativa: Especificação: Utilizar certificado X.509 para a assinatura de e-mail, quando exigido. As autoridades certificadoras raiz ou intermediárias são as responsáveis por gerar o certificado X.509, elas seguem uma série de padrões definida pela ICP-Brasil, que é a infra-estrutura de chaves públicas brasileira.

Os padrões da ICP-Brasil são bastante rígidos no que diz respeito à identidade do dono do certificado, por isso é uma boa opção para a assinatura de um e-mail, garantindo com eficiência a autenticidade, a confidencialidade e o não-repúdio da mensagem.

Responsável: Andre Bereza Junior

Enviada em: 16/11/2007 16:54

RESPOSTA:

Caro Senhor Andre,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, o grupo considerou que o Componente “Assinatura” da Tabela 4 – Especificações Técnicas para Segurança de Correio Eletrônico já contempla a sugestão apresentada.

Atenciosamente,

Coordenador do GT2 da e-PING

10) CONTRIBUIÇÃO:

Sugiro a adoção dos algoritmos Blowfish e Twofish como algoritmo de cifração (tabela 5 do documento de referência).

Justificativa: Ao meu ver, como o Blowfish é livre de patentes e de domínio público, se enquadra no espírito que levou o e-ping a preferir soluções livres.

Responsável: Felipe Alexandre Ferreira

Enviada em: 16/11/2007 16:55

RESPOSTA:

Caro Senhor Felipe,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, resolveu-se não aceitar a inclusão dos algoritmos Blowfish e Twofish em razão de realizarem a mesma função que o AES. Apesar estarem colocados pelos autores em domínio público, faltaria também ao Blowfish e ao Twofish uma entidade de caráter público que o mantenha, que é uma premissa utilizada na e-PING.

Atenciosamente,

Coordenador do GT2 da e-PING

11) CONTRIBUIÇÃO:

A contribuição a seguir se refere ao Documento de Referência da e-PING ? Versão 2.9, item 7.2. Segurança: Especificações Técnicas, Tabela 4 ? Especificações Técnicas para Segurança de Correio Eletrônico.

Componente: Assinatura

Justificativa: Especificação: Utilizar certificado X.509 para a assinatura de e-mail, quando exigido. As autoridades certificadoras raiz ou intermediárias são as responsáveis por gerar o certificado X.509, elas seguem uma série de padrões definida pela ICP-Brasil, que é a infra-estrutura de chaves públicas brasileira.

Os padrões da ICP-Brasil são bastante rígidos no que diz respeito à identidade do dono do certificado, por isso é uma boa opção para a assinatura de um e-mail, garantindo com eficiência a autenticidade, a confidencialidade e o não-repúdio da mensagem.

Responsável: Andre Bereza Junior

Enviada em: 16/11/2007 16:56

RESPOSTA:

Igual à resposta 9.

12) CONTRIBUIÇÃO:

Utilizar, além do 3DES e do AES, o algoritmo de ciframento Blowfish na tabela 5 do item 7.2

Justificativa: O Blowfish é um algoritmo de ciframento simétrico altamente difundido e de domínio público. Ele aceita chaves de 32 a 448 bits, o que o torna bastante flexível. É um dos algoritmos de criptografia mais rápidos em uso. Sugiro adicioná-lo como "recomendado".

Responsável: João Eduardo Hornburg

Enviada em: 16/11/2007 19:18

RESPOSTA:

Igual à resposta 8.

13) CONTRIBUIÇÃO:

item 7.2. Tabela 4 "Especificações Técnicas para Segurança de Correio Eletrônico.

Componente: Assinatura

Especificação: Utilizar certificado X.509 para a assinatura de e-mail, quando exigido.

Justificativa: As autoridades certificadoras raiz ou intermediárias são as responsáveis por gerar o certificado X.509, elas seguem uma série de padrões definida pela ICP-Brasil, que é a infraestrutura de chaves públicas brasileira.

Os padrões da ICP-Brasil são bastante rígidos no que diz respeito à identidade do dono do certificado, por isso é uma boa opção para a assinatura de um e-mail, garantindo com eficiência a autenticidade, a confidencialidade e o não-repúdio da mensagem.

Responsável: Andre Bereza Junior

Enviada em: 16/11/2007 22:10

RESPOSTA:

Igual à resposta 9.

14) CONTRIBUIÇÃO:

Na tabela 9 - Especificações Técnicas para Segurança "Coleta, Tratamento e Arquivamento de

Evidências.

Justificativa: O Brasil é um país que ainda carece de uma legislação específica para crimes virtuais. Mesmo sendo o melhor a se fazer, é um processo bastante lento. Ao invés de procurar e simplesmente tentar aplicar modelos e padrões internacionais que são amparados pela legislação local de cada país, deve-se criar um modelo específico para que a coleta, tratamento e arquivamento de evidências seja otimizado para lembrando que tais crimes são na sua grande maioria encaixados no atual código penal.

E, em seguida, adicionar um item com especificação "Estudo Futuro", para o desenvolvimento ou mesmo adaptação desse modelo em conformidade e paralelamente à criação de uma eventual legislação específica.

Responsável: Diego Rodrigues Machado

Enviada em: 16/11/2007 23:56

RESPOSTA:

Caro Senhor Diego,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, o GT2 considerou que a questão é técnica e não jurídica. A idéia é oferecer uma metodologia amplamente aceita e que contenha os principais elementos necessários para lidar com situações que um incidente de segurança da informação possa ser analisado com mais profundidade, para atender a objetivos da organização. Por isso, no momento a sugestão não será acatada, porém, o estudo de metodologia própria poderá ser analisado futuramente.

Atenciosamente,

Coordenador do GT2 da e-PING

15) CONTRIBUIÇÃO (encaminhada via e-mail):

Sou participante do GT-2 e sugiro a inclusão de item referente a estudo que já estou desenvolvendo sobre os "Padrões recomendados para Planos de Recuperação de Desastre e Continuidade Operacional no Governo". Sou membro do Grupo de Contingência do SERPRO, especialista em Segurança e Gestão de Planos de Continuidade de Negócios certificado pelo Disaster Recovery Institute International nos EUA (www.drii.org), mestrado em Administração e Gestão de Produtividade Organizacional pela FACECA e pós-graduado pela FGV. Atenciosamente. Antonio.

Responsável: Antonio Acras Filho

Enviada em: 14/11/2007 08:48

RESPOSTA:

Caro Senhor Antonio,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, aguardaremos a contribuição em concreto, pois não foi encaminhado material para discussão pelo GT2. Sugerimos a participação pessoalmente em reuniões do GT2, bastaria se comunicar com a organização da e-PING.

Atenciosamente,

Coordenador do GT2 da e-PING

16) CONTRIBUIÇÃO (encaminhada via e-mail):

Bom dia

Gostaria de fazer uma pequena contribuição com algumas idéias sobre os possíveis usos de uma VPN e sobre o algoritmo de criptografia simétrica AES.

O documento em anexo contém um texto básico falando sobre o assunto.

Obrigado

Olhando a seção 7.2(Segurança: Especificações Técnicas), na tabela 3, seção que fala sobre a transferência de dados em redes inseguras há um item que menciona alguns algoritmos para definição de chave de cifração. Ali estão listados RC4, IDEA e o 3DES. Eu gostaria de propor também, e principalmente, o uso do AES (Advanced Encryption Standard # Padrão de Ciframento Avançado).

Esse algoritmo foi desenvolvido após a abertura, pelo governo norte-americano, de uma consulta pública para um algoritmo de criptografia simétrica que viria a substituir o DES, padrão na época. Após anos de desenvolvimento e análise ele foi aceito como o padrão para ciframento de informações do governo norte-americano e vem sendo cada vez mais adotado como padrão em todo o mundo.

Acredito que por ser um algoritmo desenvolvido recentemente, e por ter a sua segurança comprovada e uma estimativa de vida mais longa que os algoritmos citados, é uma boa escolha para ser inserido nesse conjunto de algoritmos de ciframento.

Responsável: Rafael Meneguzzo Sartor

Enviada em: 16/11/2007 10:26

RESPOSTA:

Caro Senhor Rafael,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, o GT2 aceitou a sugestão, considerando que um erro material, deixou-se de incluir o algoritmo AES na Tabela 3 - Especificações Técnicas para Segurança de IP, apesar de tê-lo incluído na Tabela 5 – Especificações Técnicas para Segurança – Criptografia.

Atenciosamente,
Coordenador do GT2 da e-PING

Respostas Relativas ao GT – Meios de Acesso

01) CONTRIBUIÇÃO:

Gostaria de reforçar a sugestão do colega Daniel Fernandes (SERPRO/TIFLA) que sugeriu a promoção do formato ODF para o status de Adotado.

Justificativa: O impacto desta medida não seria impedimento a meu ver, uma vez que grande parte dos documentos produzidos no governo hoje não está no formato Adotado, muito menos em formato Recomendado, e sim no formato MicroSoft-Office que tem status Transitório.

Responsável: Emmanuel Nazareno de Lima Ferro

Enviada em: 13/11/2007 17:47

RESPOSTA:

Caro Senhor Emmanuel,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Quanto ao seu questionamento, consideramos prematura a homologação do ODF como um formato adotado neste momento. O formato ODF contribui efetivamente para a interoperabilidade entre sistemas e atende às políticas gerais da e-PING, especialmente no que diz respeito à adoção preferencial de padrões abertos. Entendemos entretanto que o impacto de sua adoção é considerável, justamente devido à prevalência de outros formatos proprietários, devendo ser objeto de estudo cuidadoso. Reconhecemos as vantagens oferecidas pelo formato ODF e continuaremos avaliando a possibilidade de sua homologação futura.

Atenciosamente,

Coordenador do GT3 da e-PING

2) CONTRIBUIÇÃO:

Reforço minha fala durante a consulta pública realizada no SERPRO, em 13/11/2007, para que os formatos ODF (Open Document Format - odt, ods, odp e odb) sejam classificados como "Adotado (A)".

Justificativa: Os formatos ODF são padrão ISO/IEC 26300 (padrão aberto, conforme orientação do E-PING) e são utilizados por uma boa gama de aplicativos de escritórios livres, entre os quais

destaca-se o OpenOffice.org/BrOffice.org. Além disso, por possibilitarem formatações complexas, são claramente mais adequados que os formatos "texto puro", atualmente classificados como "Adotado". Essa classificação seria ainda uma forma de incentivar ainda mais o uso de software livre pelos órgãos de governo.

Responsável: Daniel Lima Fernandes

Enviada em: 14/11/2007 19:39

RESPOSTA:

Caro Senhor Daniel,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Quanto ao seu questionamento, consideramos prematura a homologação do ODF como um formato adotado neste momento. O formato ODF contribui efetivamente para a interoperabilidade entre sistemas e atende às políticas gerais da e-PING, especialmente no que diz respeito à adoção preferencial de padrões abertos. Entendemos entretanto que o impacto de sua adoção é considerável, devido à prevalência de outros formatos proprietários, devendo ser objeto de estudo cuidadoso. Reconhecemos as vantagens oferecidas pelo formato ODF e continuaremos avaliando a possibilidade de sua homologação futura.

Como o foco da e-PING é a interoperabilidade, julgamos absolutamente justificada a adoção dos formatos de "texto puro". Documentos nesses formatos podem ser manipulados por todos os aplicativos de escritório e em quaisquer sistemas operacionais. Aplicações desenvolvidas pelos diversos órgãos de governo podem implementar facilmente a leitura e geração desses documentos. Entendemos que documentos em "texto puro" não competem com os formatos "ricos" (como o ODF e outros) e devem ser preferíveis sempre que suas limitações não sejam um impedimento importante.

Atenciosamente,

Coordenador do GT3 da e-PING

3) CONTRIBUIÇÃO:

Garantir o acesso às informações a partir de qualquer browser.

Justificativa: A adoção de navegadores (browsers) como principal meio de acesso a dados na e-PING tem um caráter prático e deve facilitar a utilização das informações trocadas com base no

padrão e-PING. Essa recomendação coincide com a terceira recomendação da e-GIF britânica ? adoption of the browser as the key interface. Há, entretanto, dois pontos a destacar quanto a essa recomendação:

1. Na recomendação britânica, os navegadores são adotados como centrais para a interatividade dos sistemas de informação, sem exceção. No texto da recomendação britânica encontramos a única seguinte ressalva: ?other interfaces are permitted but only in addition to browser-based ones?. Essa recomendação foi alterada na especificação brasileira, tornando-se mais permissiva: ?outras interfaces são permitidas em situações específicas, como em rotinas de atualização e captura de dados onde não haja alternativa tecnológica disponível baseada em navegadores?. Consideramos essa permissividade adicional desnecessária.

2. Tanto na recomendação britânica como na brasileira não são especificadas as funcionalidades dos navegadores que serão utilizadas. Para garantir a interoperabilidade, é importante normatizar que sejam utilizadas apenas as funcionalidades presentes em todos os navegadores existentes e disponíveis para uso.

Responsável: Flavio Soares Correa da Silva

Enviada em: 15/11/2007 17:40

RESPOSTA:

Caro Senhor Flavio,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Quanto ao seu questionamento, devemos explicar os objetivos do documento em relação aos dois itens mencionados.

1. Entendemos que a permissão mencionada é concedida mediante uma restrição bastante forte (“onde não haja alternativa tecnológica disponível baseada em navegadores”) e não pode ser confundida com permissividade. O item em questão diz respeito a situações específicas que não podem ser negligenciadas e, exatamente por esse motivo, o documento da e-PING prevê adoção gradual pelos órgãos governamentais. A alteração proposta exige uma avaliação cuidadosa que não poderá ser contemplada ainda na presente versão, mas será objeto de consideração futura.
2. A segunda alteração proposta implicaria em que fossem identificadas as funcionalidades comuns a todos os navegadores ou, para que fosse factível, pelo menos daqueles que são mais utilizados. Para que o efeito normativo sugerido não resultasse impreciso e pouco efetivo, seria necessário especificar os navegadores e versões mínimas que implementam as funcionalidades identificadas. Desde a versão 2.0 do presente documento, optamos por não especificar navegadores e versões. Existem organizações, destacadamente o *World Wide*

Web Consortium (W3C), dedicadas ao trabalho de padronização para a Web. Embora ainda existam pequenas divergências quanto à implementação dos chamados *padrões Web*, todos os principais navegadores têm evoluído continuamente em busca da aderência a esses padrões. É claro que os navegadores ainda implementam funcionalidades adicionais, muitas vezes baseadas em tecnologias proprietárias e incompatíveis com outros navegadores. Assim, preferimos realizar a prescrição de um padrão mínimo de navegador indiretamente, por meio da exigência de suporte aos padrões Web relacionados na tabela 10. Pretendemos reavaliar continuamente a efetividade da presente abordagem de modo a promover ajustes e alterações que se façam necessárias em futuras versões do documento.

Atenciosamente,
Coordenador do GT3 da e-PING

4) CONTRIBUIÇÃO:

Especificar os recursos dos browsers que serão utilizados na e-PING.

Justificativa: A adoção de navegadores (browsers) como principal meio de acesso na e-PING tem um caráter prático e deve facilitar a utilização das informações trocadas com base no padrão e-PING. Essa recomendação coincide com a terceira recomendação da e-GIF britânica ? adoption of the browser as the key interface. Há, entretanto, dois pontos a destacar quanto a essa recomendação:

1. Na recomendação britânica, os navegadores são adotados como centrais para a interatividade dos sistemas de informação, sem exceção. No texto da recomendação britânica encontramos a única seguinte ressalva: ?other interfaces are permitted but only in addition to browser-based ones?. Essa recomendação foi alterada na especificação brasileira, tornando-se mais permissiva: ?outras interfaces são permitidas em situações específicas, como em rotinas de atualização e captação de dados onde não haja alternativa tecnológica disponível baseada em navegadores?. Consideramos essa permissividade adicional desnecessária.

2. Tanto na recomendação britânica como na brasileira não são especificadas as funcionalidades dos navegadores que serão utilizadas. Para garantir a interoperabilidade, é importante normatizar que sejam utilizadas apenas as funcionalidades presentes em todos os navegadores existentes e disponíveis para uso.

Responsável: Flavio Soares Correa da Silva
Enviada em: 15/11/2007 18:22

RESPOSTA:

Igual à resposta 3.

5) CONTRIBUIÇÃO (encaminhada via e-mail):

Incluir a os formatos Ecma 376 - Office Open XML como Recomendado para padrões de documentos.

Justificativa:

Os padrões classificados e apresentados na tabela 10 merecem uma revisão cuidadosa, para se tornarem compatíveis com a qualidade das especificações apresentadas nas demais tabelas. Essa tabela foi construída, aparentemente, tomando como base a tabela 6 do documento Technical Standards Catalogue, Versão 6.2, que faz parte da documentação do e-GIF britânico. Há diferenças significativas, entretanto, entre essas duas tabelas. A tabela 6 do Technical Standards Catalogue é bastante concisa, genérica e tem caráter claramente inclusivo – ao final das listas de formatos adotados é incluída uma cláusula que acrescenta dentre os padrões e formatos adotados “quaisquer outros padrões possam ser utilizados além dos considerados explicitamente nesse documento, desde que eles atendam às políticas técnicas propostas pela e-GIF”; a tabela 10 da Referência e-PING não só não inclui cláusulas semelhantes a essa, mas ainda discrimina certos formatos e padrões classificando-os como Em Transição, sem explicação de qual política técnica não estaria sendo atendida.

Alguns padrões e formatos altamente difundidos, como os baseados no Ecma Office Open XML não constam da tabela 10. Certos padrões e formatos na categoria Recomendado, por outro lado, ainda são pouco utilizados. Independentemente dos méritos técnicos dos diferentes formatos e padrões, consideramos que o princípio de minimizar as exigências de padronização para ampliar o alcance da interoperabilidade – que é afinal o objetivo desse projeto – deve conduzir a que se evite privilegiar alguns formatos e padrões em detrimento de outros. Considerando o interesse multilateral de acesso a dados e serviços – ou seja, considerando que o projeto do Governo Eletrônico deve criar canais eficazes para o diálogo entre o governo federal e os cidadãos e as empresas, em que informações e serviços importantes serão oferecidos para a população e as empresas e também pela população e as empresas para o governo – a atitude inclusiva aplicada aos formatos e padrões de dados e serviços merece ainda mais ênfase.

Além do formato básico de transmissão de informações do Ecma Office Open XML, fundamentado em XML nautalmente, são propostos esquemas de codificação de informações desenvolvidos especificamente para a codificação de documentos de texto, planilhas, arquivos de apresentação, tabelas de dados e arquivos multimídia. A inclusão de alguns esquemas específicos e a não inclusão de outros – de qualidade reconhecidamente equivalente aos incluídos e credenciados por organismos de especificação também internacionalmente reconhecidos, como é o caso do Ecma International – pode produzir efeitos de indução que favoreçam certas comunidades de desenvolvimento de sistemas – e conseqüentemente certas empresas e grupos de usuários – em detrimento de outras, novamente contrariando o princípio básico dessa iniciativa, que é o de ampliar o alcance da interoperabilidade.

Há duas possibilidades para sanar essas deficiências observadas no Documento de Referência e-

PING conforme se apresenta nesse momento:

1. Evitar a referência a esquemas específicos na e-PING, dessa forma assumindo uma posição de neutralidade e se aproximando do ideal de minimização das exigências de padronização, e enfatizar que os formatos e padrões citados nas tabelas de especificação devem ser complementados por – parafraseando a e-GIF britânica – “quaisquer outros padrões, desde que atendam às políticas técnicas propostas pela Referência e-PING”; ou

2. Efetuar uma consulta ampla aos produtores de sistemas de informação, usuários e provedores de informações, para que, ao colocar em operação a arquitetura e-PING, suas tabelas de padrões e formatos explicitamente indicados sejam as mais representativas dos interesses desses três grupos. Nesse caso, também se deve explicitar que as tabelas devem ser complementadas por “quaisquer outros padrões, desde que atendam às políticas técnicas propostas pela e-PING”, ou alternativamente, incluir a norma Ecma 376 - Office Open XML.

Em qualquer das possibilidades, devem ser adotados princípios comuns às metodologias de desenvolvimento de sistemas para interoperabilidade, que incluem a minimização da intrusão nos procedimentos pré-existentes de processamento de informação. Dessa forma, padrões e formatos amplamente utilizados devem ter seu suporte garantido. Seguindo o modelo da documentação da e-GIF britânica, a utilização da categoria T – Em Transição, poderia ser suprimida ou pelo menos utilizada com extrema parcimônia.

Concretamente, a Referência e-PING deve passar ao largo da polêmica formada devido à contraposição de dois padrões existentes para a codificação de documentos de texto, planilhas, arquivos de apresentação, tabelas de dados e arquivos multimídia:

1. O OpenDocument Format – ODF – originário da OASIS (Organization for the Advancement of Structured Information Standards), que é um consórcio internacional sem fins lucrativos que conta com aproximadamente seiscentas organizações associadas, dentre elas a IBM e a Sun Microsystems Inc. O OpenDocument Format é baseado em formatos de dados desenvolvidos para a OpenOffice Office Suite, que é um pacote de software de código aberto que por sua vez se baseia no produto denominado StarOffice, atualmente de propriedade da Sun Microsystems Inc. Mesmo assim o OpenDocument Format proposto pela OASIS foi reconhecido pela ISO (International Organization for Standardization), como um padrão internacional.

2. O Office Open XML – OOXML – inicialmente proposto pela Microsoft Corporation, e adotado em sua última versão do produto Microsoft Office 2007. O padrão Office Open XML é reconhecido pela ECMA International (<http://www.ecma-international.org>) e está em processo de análise pela ISSO, já tendo passado pela primeira fase de votação em Setembro de 2007 e a segunda fase vai ocorrer em fevereiro de 2008. Portanto, a ISO está prestes a reconhecer o Open XML como um padrão internacional, tal qual fez com o ODF.

É cabível observar ser essencialmente inevitável que, padronizações à parte, diferentes grupos de usuários continuem a usar diferentes produtos para manipulação de documentos. Como consequência, as organizações interessadas em maximizar a acessibilidade e utilidade de seus dados – dentre as quais deve constar a iniciativa do Governo Eletrônico – devem adotar e procurar conciliar os dois padrões.

A proposta de usuários e fornecedores de informações precisarem optar por um padrão de formatação de documentos em detrimento de outros não parece ser a melhor alternativa para os próprios usuários e fornecedores de informações. Ela certamente atende interesses de produtores e fornecedores de software para produção e utilização de documentos, e parece natural que os produtores e vendedores ou distribuidores/disseminadores de um software específico enalteçam as qualidades de seu produto e do padrão de formatação de dados que o acompanha, ignorando seus pontos fracos. Esse comportamento, embora natural, não se mostra completamente adequado para esclarecer os usuários e fornecedores de informações, para que eles possam fundamentar suas decisões da maneira mais adequada.

No caso específico de padrões para codificação de documentos, a alternativa mais vantajosa para os produtores e consumidores desses documentos é incentivar a coexistência de uma pluralidade controlada de padrões, acompanhada do desenvolvimento de ferramentas apropriadas para a migração irrestrita entre padrões, maximizando dessa forma a interoperabilidade entre sistemas e fontes de informação. Uma eventual contraposição dos dois padrões não deve levar seus proponentes a construir mecanismos que constituam barreiras à sua evolução de formatos de codificação.

Concretamente no que diz respeito à arquitetura e-PING, que existe para garantir e promover a interoperabilidade com e dentro do Governo Eletrônico, a amplitude de consideração de padrões é uma qualidade a ser buscada permanentemente. Não existe fundamentação técnica que justifique a exclusão de qualquer um desses dois padrões como Recomendado na Referência e-PING. A polêmica que tem construído artificialmente uma condição de enfrentamento entre esses padrões não deveria influenciar a Referência e-PING, e a isenção do corpo técnico responsável por esse documento se comprovaria por uma consideração homogênea dos dois padrões na documentação da arquitetura e-PING.

Responsável: Raimundo Nonato da Costa

Enviada em: 15/11/2007 19:14

RESPOSTA:

Caro Senhor Raimundo,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING. Seguem abaixo nossas considerações com relação aos seus questionamentos.

O proponente defende que a tabela 10 do documento deveria ser alterada, de modo a incluir

adicionalmente os formatos *Office Open XML* (OOXML), com status similar àquele conferido aos do *Open Document Format* (ODF) – “RECOMENDADO”. Os argumentos utilizados baseiam-se fundamentalmente em que a e-PING deveria possuir o mesmo caráter inclusivo da e-GIF britânica.

Inicialmente, foi feita uma comparação entre abordagens adotadas pela e-GIF britânica e a e-PING. A documentação da e-GIF serviu concretamente de referência para os trabalhos realizados pelo Governo Federal Brasileiro na elaboração de sua plataforma de interoperabilidade. Ao buscar as melhores práticas e tendo sido reconhecida a e-GIF como uma das melhores iniciativas mundiais sobre o tema, ela foi estudada em profundidade e subsidiou a elaboração do Documento de Referência da e-PING – Versão 0. Desde aquela versão, porém, foram observadas as peculiaridades e especificidades da Administração Pública brasileira, bem como as Políticas Públicas destinadas à TIC no Brasil, em muito diferentes da realidade britânica, por conseguinte, acarretando naturais diferenças nos dois documentos comparados pelo proponente. Ademais, a evolução do Documento de Referência da e-PING em suas versões posteriores, por via de processo amplamente aberto e participativo do governo e da sociedade brasileiros, acentuou ainda mais as características intrínsecas à realidade nacional, de modo a marcar ainda mais algumas opções feitas na e-PING quando comparadas à e-GIF.

Isso justifica a diferença destacada pelo proponente entre a Tabela 6 da e-GIF e a Tabela 10 da e-PING. A Tabela 10 retrata a opção feita pelo governo brasileiro, de acordo com as políticas públicas estabelecidas para a área de Tecnologia da Informação e Comunicação, retratadas nas Políticas Gerais da e-PING. Portanto, se no Reino Unido entenderam que é interessante ser o mais permissivo e inclusivo possível, no Brasil entendemos que é importante delimitar as fronteiras das TIC de modo a ter melhor domínio e controle sobre a interoperabilidade dos serviços de governo eletrônico.

O proponente afirma ainda que o corrente documento discrimina determinados padrões classificando-os como aceitos transitoriamente. Enfatizamos que não se trata de discriminação. Quando um padrão é classificado com o status “EM TRANSIÇÃO”, está-se tão somente informando que, conforme disposto nas Políticas Gerais da e-PING, tal especificação, por ser de natureza “proprietária”, será aceita transitoriamente até que sua migração para outra de natureza “aberta” seja factível.

A e-PING não descarta de antemão quaisquer iniciativas destinadas a promover a interoperabilidade. Nesse sentido, embora julgemos prematuro incluir neste momento os formatos OOXML, continuaremos acompanhando e avaliando essa possibilidade em versões futuras. Estaremos especialmente atentos ao seu trâmite na *International Standards Organization* (ISO).

Atenciosamente,
Coordenador do GT3 da e-PING

Respostas Relativas ao GT – Organização e Intercâmbio de Informações

01) CONTRIBUIÇÃO:

Especificar melhor o uso esperado de UML como linguagem para organização e intercâmbio de informações, ou então retirar essa linguagem do documento.

Justificativa: A inclusão de UML ? Unified Modeling Language ? como padrão para definição de dados para intercâmbio é imprecisa e dá margem para interpretações diversificadas. UML é uma linguagem diagramática dirigida à especificação e projeto de sistemas computacionais, em vez de dados e serviços. Essa linguagem é composta por diversos diagramas, com recursos e significados diversos. Alguns desses diagramas talvez possam ser utilizados para especificar dados e serviços a serem comunicados e transferidos entre sistemas, ainda nesse caso divergindo significativamente de sua utilização originalmente pretendida (conforme demonstra a literatura tradicional de Engenharia de Software que apresenta a linguagem de especificação UML). As especificações precisas de quais diagramas da linguagem UML possam e devam ser utilizados, e de que forma, é um requisito importante para garantir a precisão da Referência e-PING.

A linguagem UML, adicionalmente, se presta com maior eficiência ao projeto e especificação de sistemas orientados a objetos. Embora essa metodologia de projeto e desenvolvimento de sistemas predomine atualmente na indústria de software, ela não é a única nem necessariamente a mais apropriada para a especificação de dados e serviços informacionais. A inclusão de uma ressalva de que o uso dessa linguagem é recomendado quando cabível, considerando a metodologia de desenvolvimento de sistemas utilizada, pode salvaguardar a qualidade dos procedimentos relevantes para o Governo Eletrônico.

Responsável: Flavio Soares Correa da Silva

Enviada em: 15/11/2007 17:24

RESPOSTA:

Caro Senhor Flavio,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, possivelmente quando a Parte 2 do Catálogo de Padrão de Dados (CPD) for publicada, a forma de utilização da UML fique esclarecida, porém consideramos a sua contribuição relevante e será fruto de discussão e estudos do Grupo 4.

Atenciosamente,

Coordenador do GT4 da e-PING

2) CONTRIBUIÇÃO:

Prever a análise de iniciativas similares no que se refere a esquemas de metadados e ontologias, para garantir que a e-PING se manterá alinhada a iniciativas similares internacionais.

Justificativa: A arquitetura e-PING tem sido amadurecida e ampliada no que se refere à padronização semântica das informações, conforme fica evidente ao apreciarmos a evolução desse aspecto nas diferentes versões do documento de Referência da e-PING. Ainda existem, entretanto, oportunidades para aperfeiçoamento significativo da e-PING quanto a esse aspecto. Certamente uma análise criteriosa dessa questão deve ser objeto de avaliações futuras.

A Lista de Assuntos do Governo influi diretamente nos esquemas de metadados adotados na Referência e-PING e, portanto, a interdependência entre esses itens deve ser apresentada de forma explícita.

Considerando aspectos de globalização econômica e construção de mercados comuns ? em especial os referentes à integração latino-americana ? o alinhamento dos padrões apresentados nesse item da Referência e-PING com os de iniciativas semelhantes de outros governos é fator essencial para garantir a qualidade dos padrões de interoperabilidade propostos pelo Governo Eletrônico.

Responsável: Flavio Soares Correa da Silva

Enviada em: 15/11/2007 17:29

RESPOSTA:

Caro Senhor Flavio,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, informamos que o GT4 tem acompanhado as iniciativas similares de outros países na área governamental ou mesmo acadêmica.

Estamos cientes da necessidade de evoluir a LAG. No momento estamos estudando estratégias para encontrar o caminho da evolução. Certamente somente o aperfeiçoamento da lista com inclusão de novos termos e reestruturações não é a evolução que desejamos. Quanto a interdependência entre a taxonomia e o Padrão de Metadados em desenvolvimento, creio que ficará explícita com a publicação do Padrão de Metadados.

Quanto aos aspectos de globalização e em especial a integração latino-americana, informamos que durante o corrente ano, estivemos reunidos com representantes da CEPAL (Comissão Econômica para América-Latina e Caribe) discutindo a possibilidade do desenvolvimento de projeto piloto com base na e-PING. Elaboramos também com o governo Argentino uma proposta de cooperação-técnica Brasil-Argentina no tocante a interoperabilidade de governo eletrônico.

Atenciosamente,
Coordenador do GT4 da e-PING

Respostas Relativas ao GT – Áreas de Integração para Governo Eletrônico

1) CONTRIBUIÇÃO:

Correção da definição de GeoTIFF que consta em "Observações" na página 39.

Justificativa: Um erro grosseiro foi incluído nas últimas versões do e-PING: GeoTIFF é um dado matricial e NÃO vetorial como foi incluído no e-PING.

Responsável: Helton Uchoa

Enviada em: 16/11/2007 22:33

RESPOSTA:

Caro Senhor Helton,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, já havia sido verificado este erro na versão 2.9, mas por algum engano na atualização do documento, não foi implementada. Sua contribuição será incorporada e a versão 2.9 será devidamente corrigida.

Atenciosamente,

Coordenadora do GT5 da e-PING

2) CONTRIBUIÇÃO:

Correção da definição de GeoTIFF que consta em "Observações" na página 39.

Justificativa: Um erro grosseiro foi incluído nas últimas versões do e-PING: GeoTIFF é um dado matricial e NÃO vetorial como foi incluído no e-PING.

Responsável: Helton Uchoa

Enviada em: 16/11/2007 22:34

RESPOSTA:

Igual à resposta 1.

3) CONTRIBUIÇÃO:

O formato Shapefile é propriedade da ESRI. O sua especificação foi disponibilizada na internet, mas a propriedade continua sendo desta empresa. Desta forma, em documentos oficiais é importante destacar a propriedade do mesmo

Justificativa: Da forma como foi colocado no e-PING, não está claro a questão da propriedade do formato, podendo gerar processos contra o governo.

Responsável: Helton Uchoa

Enviada em: 16/11/2007 22:37

RESPOSTA:

Caro Senhor Helton,

obrigado por contribuir no processo de aperfeiçoamento da versão 2.9 do documento de referência da e-PING.

Relativo ao seu questionamento, o formato shapefile para arquivos individuais, de intercâmbio de dados (flat files) é o mais utilizado, e mesmo tendo nascido de uma proposição de uma empresa particular, isso não obriga sua citação, devido ao seu largo uso. É considerado um formato aberto e existe um grande número de produtos que codificam e decodificam arquivos de formato shapefile, cuja estrutura não é modificada a muito tempo.

Atenciosamente,

Coordenadora do GT5 da e-PING