Declaração de Práticas de Carimbo do Tempo da Autoridade de Carimbo do Tempo Certisign

DPCT da ACT CERTISIGN

Versão 1.2- 19/12/2017

Sumário

CONTROLE DE ALTERAÇÕES

Versão	Data	Resolução que a provou a alteração	Item Alterado	Descrição da Alteração
1.1	**20/05/2016**	**Não se aplica**	1.4, 4.1.2, 4.4.8, 4.4.9, 6.4, 6.7.2, 6.8.1, 6.8.2, 6.9.1, 6.9.2, 6.9.3, 6.9.4, 6.9.5	Revisão da ordenação dos parágrafos
1.2	**19/12/2017**	**Não se aplica**	1.4; 4.5.2; 6.1.6; 6.2; 6.4; 6.5; 6.6; 6.7; 6.8; 6.9; 6.10; 6.11; 7.2.1.; 8.1; 8.2; 10	Adequação à versão 1.2 do DOC-ICP-12
		Resolução 119, de 06/07/2017	2.7.1	Referência a auditoria WEBTRUST

1. INTRODUÇÃO

1.1. Visão Geral

1.1.1. Um carimbo do tempo aplicado a uma assinatura digital ou a um documento prova que ele já existia na data incluída no carimbo do tempo. Os carimbos de tempo são emitidos por terceiras partes confiáveis, a ACT Certisign tem suas operações devidamente documentadas e periodicamente auditadas pela própria AC-Raiz da ICP-Brasil. Os relógios dos SCTs são auditados e sincronizados por Sistemas de Auditoria e Sincronismo (SASs).

1.1.2. A utilização de carimbos de tempo no âmbito da ICP-Brasil é facultativa. Documentos eletrônicos assinados digitalmente com chave privada correspondente a certificados ICP-Brasil são válidos com ou sem o carimbo do tempo.

1.1.3. Este documento estabelece os requisitos mínimos a serem obrigatoriamente observados pela ACT Certisign, integrante da ICP-Brasil na elaboração de sua Declaração de Práticas de Carimbo do tempo (DPCT). Esta DPCT descreve as práticas e os procedimentos empregados pela ACT Certisign na execução de seus serviços. De modo geral, a política de carimbo do tempo indica "o que deve ser cumprido" enquanto uma declaração de práticas da ACT Certisign indica "como cumprir", isto é, os processos que serão usados pela ACT Certisign para criar carimbos do tempo e manter a precisão do seu relógio.

1.1.4. Este documento tem como base as normas da ICP-Brasil, as RFC 3628 e 3161, do IETF e o documento TS 101861 do ETSI.

1.1.5. A estrutura desta DPCT está baseada no DOC-ICP-12 do Comitê Gestor da ICP-Brasil – REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL [12]. As referências a formulários presentes nesta DPCT deverão ser entendidas também como referências a outras formas que a ACT Certisign ou entidades a ela vinculadas possa vir a adotar.

1.1.6. Aplicam-se ainda à ACT Certisign e a seus Prestadores de Serviço de Suporte (PSS), no que couberem, os regulamentos dispostos nos demais documentos da ICP-Brasil, entre os quais destacamos:

a) POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4];

b) CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5];

c) CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6];

d) CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [7];

e) POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL [8];

f) REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO ÂMBITO DA ICP-BRASIL [9].

1.2. Identificação

Esta DPCT é chamada "Declaração de Práticas de Carimbo do Tempo da Autoridade de Carimbo do Tempo Certisign" e referida como "DPCT da ACT Certisign", cujo OID (*object identifier*) é 2.16.76.1.5.3.

1.3. Comunidade e Aplicabilidade

1.3.1. Autoridades de Carimbo de Tempo

Esta DPCT refere-se à ACT Certisign no âmbito da ICP-Brasil.

1.3.2. Prestador de Serviços de Suporte

1.3.2.1. Os dados a seguir, referentes às PSS utilizadas pela ACT Certisign são publicados em serviço de diretório e/ou em página web da ACT Certisign (http://icp-brasil.certisign.com.br/repositorio).

1.3.2.2. PSS são entidades utilizadas pela ACT Certisign para desempenhar atividade descrita nesta DPCT ou na PCT e se classificam em três categorias, conforme o tipo de atividade prestada:

a) disponibilização de infra-estrutura física e lógica;

b) disponibilização de recursos humanos especializados; ou

c) disponibilização de infra-estrutura física e lógica e de recursos humanos especializados.

1.3.2.3 A ACT Certisign mantém as informações acima sempre atualizadas.

1.3.3. Subscritores

Pessoas físicas ou jurídicas de direito público ou privado, nacionais ou estrangeiras, podem solicitar carimbos de tempo.

1.3.4. Aplicabilidade

A ACT Certisign implementa a seguinte Políticas de Carimbo do Tempo:

· Política de Carimbo do Tempo da Autoridade de Carimbo do Tempo Certisign, PCT da ACT Certisign, OID 2.16.76.1.6.3.

1.4. Dados de Contato

Nome:	Certisign Certificadora Digital S.A.
Endereço:	Rua Bela Cintra, 904 – 11. Andar – São Paulo
CEP:	01415-000
Área:	Normas e Compliance
Contato	Patricia T O Leite
Telefone:	(11) 4501-2417
Telefone:	(11) 4501-2436
E-mail:	icpbrasil@certisign.com.br
	normas@certisign.com.br

2. DISPOSIÇÕES GERAIS

2.1. Obrigações e Direitos

Nos itens a seguir estão descritas as obrigações gerais das entidades envolvidas. Os requisitos específicos associados a essas obrigações estão detalhados nas PCT implementadas pela ACT Certisign.

2.1.1. Obrigações da ACT Certisign

a) operar de acordo com a sua DPCT e com as PCTs que implementa;

b) gerar, gerenciar e assegurar a proteção das chaves privadas dos SCTs;

c) manter os SCTs sincronizados e auditados pela EAT;

d) tomar as medidas cabíveis para assegurar que usuários e demais entidades envolvidas tenham conhecimento de seus respectivos direitos e obrigações;

e) monitorar e controlar a operação dos serviços fornecidos;

f) assegurar que seus relógios estejam sincronizados, com autenticação, à Rede de Carimbo do Tempo da ICP-Brasil;

g) permitir o acesso da EAT aos SCTs de sua propriedade;

h) notificar à AC emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do correspondente certificado;

i) notificar as seus usuários quando ocorrer: suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;

j) publicar em sua página web sua DPCT, as PCTs aprovadas que implementa e os certificados de seus SCTs;

k) publicar, em sua página web, as informações definidas no item 2.6.1.2 deste documento;

l) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICPBrasil;

m) adotar as medidas de segurança e controle previstas na DPCT, PCT e Política de Segurança (PS) que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;

n) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;

o) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;

p) manter e testar anualmente seu Plano de Continuidade do Negócio (PCN);

q) manter contrato de seguro de cobertura de responsabilidade civil decorrente da atividade de emissão de carimbos do tempo, com cobertura suficiente e compatível com o risco dessas atividades;

r) informar às terceiras partes e subscritores de carimbos do tempo acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada nos termos acima; e

s) informar à AC-Raiz, mensalmente, a quantidade de carimbos do tempo emitidos.

2.1.2. Obrigações do Subscritor

Ao receber um carimbo do tempo, o subscritor deve verificar se o carimbo do tempo foi assinado corretamente e se a chave privada usada para assinar o carimbo do tempo não foi comprometida.

2.1.3. Direitos da Terceira Parte (Relying Party)

2.1.3.1. Considera-se terceira parte, a parte que confia no teor, validade e aplicabilidade do carimbo de tempo.

2.1.3.2 Constituem direitos da terceira parte:

a) recusar a utilização do carimbo do tempo para fins diversos dos previstos na PCT correspondente;

b) verificar, a qualquer tempo, a validade do carimbo do tempo.

2.1.3.3. Um carimbo emitido pela ACT Certisign é considerado válido quando:

a) tiver sido assinado corretamente, usando certificado ICP-Brasil específico para equipamentos de carimbo do tempo;

b) a chave privada usada para assinar o carimbo do tempo não foi comprometida até o momento da verificação;

c) caso o alvará seja integrado no CT, ele deverá também estar válido para o período do CT.

2.1.3.4 O não exercício desses direitos não afasta a responsabilidade da ACT Certisign e do subscritor.

2.2. Responsabilidades

2.2.1. Responsabilidades da ACT Certisign

2.2.1.1. A ACT Certisign responde pelos danos a que der causa.

2.2.1.2. A ACT Certisign responde solidariamente pelos atos dos PSSs por ela contratados.

2.3. Responsabilidade Financeira

2.3.1. Indenizações devidas pela terceira parte (Relying Party)

A terceira parte responde perante a ACT Certisign apenas pelos prejuízos a que der causa com a prática de ato ilícito, nos termos da legislação vigente.

2.3.2. Relações Fiduciárias

A ACT Certisign indeniza integralmente os prejuízos que, comprovadamente, der causa, prevendo o pagamento de indenização correspondente à 20 (vinte) vezes o valor do certificado, ou a R$ 40.000,00, o que for menor.

As indenizações da ACT Certisign cobrem perdas e danos decorrentes de comprometimento da chave privada da ACT Certisign, de erro na identificação do titular, de emissão defeituosa do carimbo de tempo ou de erros ou omissões da ACT Certisign.

2.3.3. Processos Administrativos

O subscritor que sofrer perdas e danos decorrentes do uso do carimbo de tempo emitido pela ACT Certisign tem o direito de comunicar à ACT Certisign que deseja a indenização prevista no item 2.3.2 acima, observadas as seguintes condições:

a) nos casos de perdas e danos decorrentes de comprometimento da chave privada da ACT Certisign, tal comprometimento deverá ter sido comprovado por perícia realizada por perito especializado e independente.

2.4. Interpretação e Execução

2.4.1. Legislação

Esta DPCT é regida pela Medida Provisória nº 2.200-02, pelas Resoluções do Comitê Gestor da ICP-Brasil, bem como pelas demais leis em vigor no Brasil.

2.4.2. Forma de interpretação e notificação

2.4.2.1. Na hipótese de uma ou mais disposições desta DPCT ser, por qualquer razão, considerada inválida, ilegal, ou conflituosa com norma da ICP-Brasil, a inaplicabilidade não afeta as demais disposições, sendo esta DPCT interpretada, então, como se não contivesse tal disposição e, na medida do possível, interpretada para manter a intenção original da DPCT. Nesse caso, o Grupo de Práticas e Políticas da ACT Certisign examinará a disposição inválida e proporá à nova redação ou retirada da disposição afetada, na forma do item 8 desta DPCT.

2.4.2.2. As notificações ou qualquer outra comunicação necessária, relativas às práticas descritas nesta DPCT, são feitas através de mensagem eletrônica assinada digitalmente, com chave pública certificada pela ICP-Brasil, ou por escrito e entregue à ACT Certisign.

2.4.3. Procedimentos da solução de disputa

2.4.3.1. Em caso de conflito entre esta DPCT da ACT Certisign, a PCT que implementa ou outros documentos que a ACT Certisign adotar, prevalece o disposto nesta DPCT. O contrato para emissão de carimbos do tempo poderá criar obrigações específicas, limitar o uso dos carimbos do tempo ou restringir valores de transações comerciais, desde que respeitados os direitos previstos nesta DPCT.

2.4.3.2. Esta DPCT da ACT Certisign não prevalece sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

2.4.3.3. Casos omissos deverão ser encaminhados para apreciação da AC Raiz.

2.5. Tarifas de Serviço

2.5.1. Tarifas de emissão e de carimbos de tempo

Variável conforme definição interna da Certisign.

2.5.2. Tarifas de acesso ao carimbo de tempo

Não são cobradas tarifas de acesso ao carimbo de tempo emitido.

2.5.3. Tarifas de revogação ou de acesso à informação de status

Variável conforme definição interna da Certisign.

2.5.4. Tarifas para outros serviços

Variável conforme definição interna da Certisign.

2.5.5. Política de reembolso

Variável conforme definição interna da Certisign.

2.6. Publicação

2.6.1. Publicação de informação da ACT Certisign

2.6.1.1. As informações descritas abaixo são publicadas em serviço de diretório e/ou em página web da ACT Certisign (http://icp-brasil.certisign.com.br/repositorio), com disponibilidade de 99,5% (noventa e nove e cinco décimos percentuais) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, obedecendo às regras e os critérios estabelecidos nesta DPCT.

2.6.1.2. As seguintes informações são publicadas em serviço de diretório e/ou em página web da ACT Certisign (http://icp-brasil.certisign.com.br/repositorio):

a) os certificados dos SCTs que opera;

b) sua DPCT;

c) as PCTs que implementa;

d) as condições gerais mediante as quais são prestados os serviços de carimbo do tempo;

e) a exatidão do carimbo do tempo com relação ao UTC;

f) algoritmos de hash que poderão ser utilizados pelos subscritores e o algoritmo de hash utilizado pela ACT;

g) uma relação, regularmente atualizada, dos PSSs vinculados.

2.6.2. Frequência de publicação

Certificados são publicados imediatamente após sua emissão. A publicação da LCR se dá conforme o item 4.4.9 da PCT correspondente. As versões ou alterações desta DPCT e da PCT são atualizadas no web site da ACT Certisign após aprovação da AC Raiz da ICP-Brasil.

2.6.3. Controles de acesso

Não há qualquer restrição ao acesso para consulta a esta DPCT, à lista de certificados emitidos, à LCR da ACT Certisign e às PCT implementadas.

São utilizados controles de acesso físico e lógico para restringir a possibilidade de escrita ou modificação desses documentos ou desta lista por pessoal não autorizado. A máquina que armazena as informações acima se encontra em nível 4 de segurança física e requer uma senha de acesso.

2.7. Fiscalização e Auditoria de Conformidade

2.7.1. As fiscalizações e auditorias realizadas na ACT Certisign e em seus PSS têm por objetivo verificar se seus processos, procedimentos e atividades estão em conformidade com suas respectivas DPCT, PCTs, PS e demais normas e procedimentos estabelecidos pela ICP-Brasil e com os princípios e critérios definidos pela WebTrust.

2.7.2. As fiscalizações da ACT Certisign e de seus PSSs são realizadas pela AC-Raiz, por meio de servidores de seu quadro próprio, a qualquer tempo, sem aviso prévio, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICPBRASIL [7].

2.7.3. As auditorias da ACT Certisign e de seus PSS são realizadas:

a) quanto aos procedimentos operacionais, pela AC-Raiz, por meio de pessoal de seu quadro próprio, ou por terceiros por ela autorizados, observado o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

b) quanto a autenticação e ao sincronismo dos SCTs pela Entidade de Auditoria do Tempo (EAT) observado o disposto no documento PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL [3].

2.7.4. A ACT Certisign recebeu auditoria prévia da AC Raiz para fins de credenciamento na ICP-Brasil e é auditada anualmente, para fins de manutenção do credenciamento, com base no disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES

INTEGRANTES DA ICP-BRASIL [6]. Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

2.7.5. As entidades da ICP-Brasil diretamente vinculadas a ACT Certisign receberam auditoria prévia da EAT, quanto aos aspectos de autenticação e sincronismo, sendo regularmente auditada, para fins de continuidade de operação, com base no disposto no documento PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS DO TEMPO NA ICP-BRASIL [3].

2.7.6. A ACT Certisign deve informar que as entidades da ICP-Brasil a ela diretamente vinculadas também receberam auditoria prévia, para fins de credenciamento, e que a ACT é responsável pela realização de auditorias anuais nessas entidades, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo 2.7.3.

2.8. Sigilo

2.8.1. Disposições gerais

2.8.1.1. ACT Certisign gera e mantém a chave privada de assinatura digital dos SCTs, sendo responsável pelo seu sigilo.

2.8.2. Tipos de informações sigilosas

2.8.2.1. Como princípio geral, todo documento, informação ou registro fornecido à ACT Certisign são sigilosos.

2.8.2.2. Nenhum documento, informação ou registro fornecido pelos titulares de carimbo de tempo à ACT Certisign será divulgado.

2.8.3. Tipos de informações não-sigilosas

As informações consideradas não-sigilosas compreendem:

a) os certificados dos SCTs;

b) as PCTs implementadas pela ACT;

c) a DPCT da ACT;

d) versões públicas de PS; e

e) a conclusão dos relatórios de auditoria.

2.8.4. Quebra de sigilo por motivos legais

A ACT Certisign fornecerá, mediante ordem judicial ou por determinação legal, documentos, informações ou registros sob sua guarda.

2.8.5. Informações a terceiros

Nenhum documento, informação ou registro sob a guarda do PSS ou da ACT Certisign é fornecido a qualquer pessoa, exceto quando a pessoa que requerer, através de instrumento devidamente constituído, estiver corretamente identificada e autorizada para fazê-lo.

2.9. Direitos de Propriedade Intelectual

A Certisign Certificadora Digital S.A. ou sua licenciante VeriSign, Inc. detém todos os direitos de propriedade intelectual sobre as idéias, conceitos, técnicas e invenções, processos e/ou obras, incluídas ou utilizadas nos produtos e serviços fornecidos pela ACT Certisign nos termos dessa DPCT.

Os Direitos de Propriedade terão proteção conforme a legislação aplicável.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1. O serviço será disponibilizado por meio do protocolo TSP (conforme descrito na RFC 3161), o cliente deve enviar uma solicitação de carimbo (timestamp query). O protocolo TSP é disponibilizado utilizando como meio de transporte protocolo HTTPS com autenticação cliente. A autenticação cliente é necessária para que o Servidor de Aplicativos identifique o subscritor e qual a sua modalidade de contabilidade.

3.2. A requisição do carimbo do tempo (TSQ) não identifica o solicitante, por isso, em situações onde a ACT precisa conhecer a identidade do solicitante devem ser usados meios alternativos de identificação e autenticação. Sendo assim o subscritor é identificado por meio do certificado digital utilizado na autenticação cliente/servidor apresentado na camada HTTPS.

4. REQUISITOS OPERACIONAIS

Como primeira mensagem deste mecanismo, o subscritor solicita um carimbo do tempo enviando um pedido (que é ou inclui uma Requisição de Carimbo do Tempo) para a ACT Certisign.

Como segunda mensagem, a ACT Certisign responde enviando uma resposta (que é ou inclui um Carimbo do Tempo) para o subscritor.

4.1. Solicitação de Carimbos do Tempo

4.1.1 Para solicitar um carimbo do tempo num documento digital, o subscritor deve enviar um TSQ (Time Stamp Request) contendo o hash a ser carimbado.

4.1.2 Para a solicitação de um carimbo de tempo são adotados os requisitos abaixo:

a) utilizar uma fonte confiável de tempo.

b) incluir um valor de tempo confiável para cada token com carimbo de tempo.

c) incluir um número inteiro único para cada carimbo de tempo recém-gerado no token.

d) produzir um carimbo de tempo no token, ao receber um pedido válido do solicitante, quando for possível.

e) incluir dentro de cada token com carimbo de tempo um identificador que indica exclusivamente a política de segurança sobre a qual o token foi criado.

f) carimbar um hash de um determinado dado.

g) examinar o OID da colisão de uma forma resistente a função hash e verificar se o comprimento do valor do hash é consistente com o algoritmo de hash.

h) não examinar o hash a ser carimbado em nenhuma hipótese, a não ser que seja para verificar seu comprimento, tal como especificado no ponto anterior).

i) não incluir qualquer identificação da entidade requerente, nos carimbos de tempo dos tokens.

j) assinar cada token carimbo de tempo usando uma chave gerada exclusivamente para este efeito e ter a propriedade da chave indicada no certificado correspondente.

k) incluir informações adicionais nos carimbos de tempo dos tokens, se perguntado pelo solicitante usando o campo de extensões, apenas para o extensões que são suportadas pela TSA. Se isto não for possível, a TSA deverá responder com uma mensagem de erro.

Para a solicitação de um carimbo de tempo são adotados os procedimentos operacionais abaixo:

O subscritor terá direito a solicitar carimbos do tempo através de solicitação no site da Certisign (http://www.certisign.com.br) ou por meio de contato com a equipe comercial/vendas. O serviço é disponibilizado por meio do protocolo TSP (conforme descrito na RFC 3161), no qual o cliente envia uma solicitação de carimbo de tempo (timestamp query) e a ACT envia uma resposta para a entidade solicitante.

A conferência do carimbo é feita pelo Sistema de Gerenciamento de ACT antes da resposta ser enviada para o subscritor. O próprio subscritor deve fazer uma segunda conferência ao receber o carimbo de tempo verificando o status de erro retornado na resposta, e se nenhum erro estiver presente deverá verificar os vários campos contidos na resposta e a validade da assinatura digital da resposta. Em particular, deve-se verificar se o que foi carimbado corresponde ao que foi solicitado.

O serviço será disponibilizado para o usuário final por meio da Internet, utilizando protocolo TSP via HTTPS com autenticação cliente, na porta 443, através do endereço https:\\act.certisign.com.br\actweb. O subscritor deve apresentar para a autenticação um certificado ICP-Brasil válido.

O acesso ao serviço deve ser feito por meio de certificado digital emitido por cadeia confiável da Certisign, configurada no serviço de ACT.

O serviço de ACT aceita hashes do tipo SHA1, SHA256, SHA384 e SHA512 e assinatura do carimbo realizado pela SCT é feito utilizando SHA1, SHA256, SHA384 e SHA512.

4.1.3. A PCT Certisign da ACT Certisign define os procedimentos específicos para solicitação dos carimbos do tempo emitidos segundo a PCT, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL [2].

4.2. Emissão de Carimbos do Tempo

4.2.1. Nos itens abaixo são descritos todos os requisitos e procedimentos operacionais referentes à emissão de um carimbo do tempo e o protocolo a ser implementado, entre aqueles definidos na RFC 3161.

4.2.2 Como princípio geral, a ACT Certisign disponibiliza aos subscritores o acesso a um Servidor de Aplicativos, para que os mesmos encaminhem as TSQs recebidas ao SCT e em seguida devolvam ao subscritor os carimbos do tempo recebidos em resposta às TSQs.

4.2.3 O Servidor de Aplicativos se constitui de um sistema instalado em equipamento da ACT Certisign distinto do SCT. O serviço disponibilizado pelo SCT é de acesso exclusivo ao servidor de aplicação da ACT.

4.2.4 O fornecimento e o correto funcionamento do Servidor de Aplicativos são de responsabilidade da ACT Certisign.

4.2.5 O Servidor de Aplicativos executa as seguintes tarefas:

a) identifica e valida, o usuário que está acessando o sistema;

b) recebe os hashes que serão carimbados;

c) envia ao SCT os hashes que serão carimbados;

d) recebe de volta os hashes devidamente carimbados;

e) confere a assinatura digital do SCT;

f) confere o hash recebido de volta do SCT com o hash enviado ao SCT;

g) confere a assinatura digital do SCT presente no carimbo do tempo;

h) confere o hash recebido de volta do SCT com o hash enviado ao SCT;

i) compara se o valor do campo nounce presente no carimbo do tempo é igual ao da TSQ enviada para a SCT;

j) devolve ao usuário o hash devidamente carimbado;

k) comuta automaticamente para o SCT reserva, em caso de pane no SCT principal;

l) emite alarmes por email aos responsáveis quando ocorrerem problemas de acesso aos SCTs.

4.2.6 O SCT, ao receber a TSQ, deve realizar a seguinte seqüência:

a) Verificar se a requisição está de acordo com as especificações da norma RFC 3161. Caso esteja, realizar as demais operações a seguir descritas. Se a requisição estiver fora das especificações, o SCT deve responder de acordo com o item 2.4.2 da RFC 3161, com um valor de status diferente de 0 ou 1, e indicar no campo "PKIFailureInfo" qual foi a falha ocorrida sem emitir, neste caso, um carimbo do tempo e encerrando, sem executar as demais etapas;

b) produzir carimbos do tempo apenas para solicitações válidas;

c) usar uma fonte confiável de tempo;

d) incluir um valor de tempo confiável para cada carimbo do tempo;

e) Incluir na resposta um identificador único para cada carimbo do tempo emitido;

f) incluir em cada carimbo do tempo um identificador da política sob a qual o carimbo do tempo foi criado;

g) somente carimbar o hash dos dados, e não os próprios dados;

h) verificar se o tamanho do hash recebido está de acordo com a função hash utilizada;

i) não examinar o hash que está sendo carimbado, de nenhuma forma, exceto para verificar seu comprimento, conforme item anterior;

j) nunca incluir no carimbo do tempo algum tipo de informação que possa identificar o requisitante do carimbo do tempo;

k) assinar cada carimbo do tempo com uma chave própria gerada exclusivamente para esse objetivo;

l) a inclusão de informações adicionais solicitadas pelo requerente deve ser feita nos campos de extensão suportados; caso não seja possível, responder com mensagem de erro;

m) encadear o carimbo do tempo atual com o anterior, caso a ACT tenha adotado o mecanismo de encadeamento.

4.2.7 A Certisign informa na PCT a disponibilidade dos seus serviços de carimbo do tempo. Essa disponibilidade deverá ser, no mínimo, de 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

4.3. Aceitação de Carimbos do Tempo

4.3.1. A solicitação de carimbo do tempo pelo subscritor ocorre por meio do uso de aplicação desenvolvida pelo cliente ou disponibilizada pela Certisign e que se comunica com o serviço de ACT. A aplicação cliente deve realizar a conferência dos dados do carimbo e deve observar os seguintes requisitos e procedimentos:

a) Verificar o valor do status indicado no campo PKIStatusInfo do carimbo do tempo. Caso nenhum erro estiver presente, isto é, o status estiver com o valor 0 (sucesso) ou 1 (sucesso com restrições), devem ser verificados os próximos itens;

b) Comparar se o hash presente no carimbo do tempo é igual ao da requisição (TSQ) que foi enviada para a ACT;

c) Comparar se o OID do algoritmo de hash no carimbo do tempo é igual ao da requisição (TSQ) que foi enviada para a ACT.

d) Comparar se o número de controle (valor do campo nounce) presente no carimbo do tempo é igual ao da requisição (TSQ) enviada para ACT;

e) Verificar a validade da assinatura digital do SCT que emitiu o carimbo do tempo;

f) Verificar se o certificado do SCT é válido e não está revogado;

g) Verificar se o certificado do SCT possui o uso adequado para este objetivo, isto é, o certificado deve possuir o valor id-kp-timeStamping com o OID definido pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [10].

4.3.2 Uma vez recebida a resposta (que é ou inclui um TimeStampResp, que normalmente contém um carimbo do tempo), o subscritor deve verificar o status de erro retornado pela resposta e, se nenhum erro estiver presente, ele deve verificar os vários campos contidos no carimbo do tempo e a validade da assinatura digital do carimbo do tempo.

4.3.3 Em especial ele deve verificar se o que foi carimbado corresponde ao que foi enviado para carimbar. O subscritor deve verificar também se o carimbo do tempo foi assinado por uma ACT credenciada e se estão corretos o hash dos dados e o OID do algoritmo de hash. Ele deve então verificar a tempestividade da resposta, analisando ou o tempo incluído na resposta, comparando-o com uma fonte local confiável de tempo, se existir, ou o valor do número de controle incluído na resposta, comparando-o com o número incluído no pedido. Se qualquer uma das verificações acima falhar, o carimbo do tempo deve ser rejeitado.

4.3.4 Além disso, como o certificado do SCT pode ter sido revogado, o status do certificado é verificado para confirmar se ainda está válido. A seguir o subscritor deve checar também o campo policy para determinar se a política sob a qual o carimbo foi emitido é aceitável ou não para a aplicação.

4.3.5 Cada PCT implementada pela ACT Certisign deve definir os procedimentos específicos para aceitação dos carimbos do tempo emitidos segundo a PCT, com base nos processos acima e nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL [2].

4.4. Procedimentos de Auditoria de Segurança

Nos itens seguintes são descritos aspectos dos sistemas de auditoria e de registro de eventos implementados pela ACT Certisign com o objetivo de manter um ambiente seguro.

4.4.1. Tipos de eventos registrados

4.4.1.1 A ACT Certisign registra em arquivos de auditoria todos os eventos relacionados à segurança do seu sistema. Entre outros, os seguintes eventos deverão obrigatoriamente estar incluídos em arquivos de auditoria:

a) iniciação e desligamento do SCT;

b) tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da ACT;

c) mudanças na configuração do SCT ou nas suas chaves;

d) mudanças nas políticas de criação de carimbos do tempo;

e) tentativas de acesso (login) e de saída do sistema (logoff);

f) tentativas não-autorizadas de acesso aos arquivos de sistema;

g) geração de chaves próprias do SCT e demais eventos

relacionados com o ciclo de vida destes certificados;

h) emissão de carimbos do tempo;

i) tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas e de atualizar e recuperar suas chaves;

j) operações falhas de escrita ou leitura, quando aplicável; e

k) todos os eventos relacionados à sincronização dos relógios dos SCTs com a FCT; isso inclui no mínimo:

i. a própria sincronização;

ii. desvio de tempo ou retardo de propagação acima de um valor especificado;

iii. falta de sinal de sincronização;

iv. tentativas de autenticação mal-sucedidas;

v. detecção da perda de sincronização.

4.4.1.2 A ACT Certisign deverá também registrar, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema, tais como:

a) registros de acessos físicos;

b) manutenção e mudanças na configuração de seus sistemas;

c) mudanças de pessoal e de perfis qualificados;

d) relatórios de discrepância e comprometimento; e

e) registros de destruição de mídias de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

4.4.1.3 Todos os registros de auditoria contêm a identidade do agente que o causou, bem como a data e horário do evento. Registros de auditoria eletrônicos contêm o horário UTC.

Registros manuais em papel poderão conter a hora local desde que especificado o local.

4.4.1.4 Esta DPCT prevê que todos os registros de auditoria contem a identidade do agente que o causou, bem como a data e horário do evento. Registros de auditoria eletrônicos contém o horário UTC. Registros manuais em papel contém a hora local desde que especificado o local

4.4.1.5 Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços da ACT Certisign é armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

4.4.2. Frequência de auditoria de registros (logs)

Esta DPCT estabelece a periodicidade, não superior a uma semana, com que os registros de auditoria da ACT Certisign são analisados pelo seu pessoal operacional. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros, com a verificação de que não foram alterados, seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas. Período de retenção para registros (logs) de auditoria Neste item, a DPCT deve estabelecer que a ACT Certisign mantenha localmente os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, deverá armazená-los da maneira descrita no item 4.5.

4.4.3. Período de retenção para registros (logs) de auditoria

Esta DPCT estabelece que a ACT Certisign mantenha localmente os seus registros de auditoria por pelo menos 2 (dois) meses e, subsequentemente, deverá armazená-los da maneira descrita no item 4.5.

4.4.4. Proteção de registro (log) de auditoria

4.4.4.1 As operações realizadas no sistema são registradas em duas camadas, na camada do servidor de aplicação, utilizando registros em arquivos (arquivo log) e em trilha de auditoria, em banco de dados.

Os eventos de auditoria armazenados em arquivo (logs) inclui mecanismos de proteção contra leitura não autorizada, modificação e remoção através das funcionalidades nativas dos sistemas operacionais. As ferramentas disponíveis no sistema operacional liberam os acessos lógicos aos registros de auditoria somente a usuários ou aplicações autorizadas, por meio de permissões de acesso dadas pelo administrador do sistema de acordo com o cargo dos usuários ou aplicações e orientação da área de segurança.

O próprio sistema operacional também registra os acessos aos arquivos onde estão armazenados os registros de auditoria.

Os registros armazenados em banco de dados possuem proteção contra atualizações que não forem realizadas pela aplicação ACT, gerando alertas para qualquer tipo de inconsistência.

4.4.4.2 Informações manuais de auditoria também são protegidas contra a leitura não autorizada, modificação e remoção através de controles de acesso aos ambientes físicos onde são armazenados estes registros.

4.4.4.3 Os mecanismos de proteção descritos obedecem à Política de Segurança da ACT Certisign, em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL.

4.4.5. Procedimentos para cópia de segurança (backup) de registro (log) de auditoria

Os registros de eventos e sumários de auditoria dos equipamentos utilizados pela ACT Certisign têm cópias de segurança semanais, feitas, automaticamente pelo sistema ou manualmente pelos administradores de sistemas. Estas cópias são enviadas ao departamento de segurança.

4.4.6. Sistema de coleta de dados de auditoria

O sistema de coleta de dados de auditoria interno à ACT Certisign é uma combinação de processos automatizados e manuais, executada por seu pessoal operacional ou por seus sistemas.

4.4.7. Notificação de agentes causadores de eventos

Quando um evento é registrado pelo conjunto de sistemas de auditoria da ACT Certisign, nenhuma notificação é enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.

4.4.8. Avaliações de vulnerabilidade

Os eventos que indiquem possível vulnerabilidade, detectados na análise periódica dos registros de auditoria da ACT Certisign, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas pela ACT Certisign e registradas para fins de auditoria.

4.5. Arquivamento de Registros

Nos itens seguintes desta DPCT é descrita a política geral de arquivamento de registros, para uso futuro, implementada pela ACT Certisign e pelos PSSs a ela vinculados.

4.5.1. Tipos de registros arquivados

a) notificações de comprometimento de chaves privadas do SCT;

b) substituições de chaves privadas dos SCTs;

c) informações de auditoria previstas no item 4.4.1.

Neste item, a DPCT deve estabelecer os períodos de retenção para cada registro arquivado, observando que os carimbos do tempo emitidos e as demais informações, inclusive arquivos de auditoria, deverão ser retidos por, no mínimo, 6 (seis) anos.

4.5.2. Período de retenção para arquivo

Os períodos de retenção para cada registro arquivado, de carimbos do tempo emitidos e das demais informações, inclusive arquivos de auditoria, são retidos por, no mínimo, 7 (sete) anos.

4.5.3. Proteção de arquivo

Todos os registros são classificados e armazenados com requisitos de segurança compatíveis com essa classificação, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

4.5.4. Procedimentos para cópia de segurança (backup) de arquivo

4.5.4.1. A ACT Certisign estabelece que uma segunda cópia de todo o material arquivado é armazenada em local externo à ACT Certisign, recebendo o mesmo tipo de proteção utilizada por ela no arquivo principal.

4.5.4.2. As cópias de segurança seguem os períodos de retenção definidos para os registros dos quais são cópias.

4.5.4.3. A ACT Certisign verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

4.5.5. Requisitos para datação (time-stamping) de registros

Informações de data e hora nos registros baseiam-se no horário Greenwich Mean Time (Zulu), incluindo segundos (no formato YYMMDDHHMMSSZ), mesmo se o número de segundos for zero.

Nos casos em que por algum motivo os documentos formalizem o uso de outro formato, ele será aceito.

4.5.6. Sistema de coleta de dados de arquivo

Todos os sistemas de coleta de dados de arquivo utilizados pela ACT Certisign em seus procedimentos operacionais são automatizados e manuais e internos.

4.5.7. Procedimentos para obter e verificar informação de arquivo

A verificação de informação de arquivo deve ser solicitada formalmente aos PSS e à ACT Certisign, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação é devidamente identificado.

4.6. Troca de chave

4.6.1. Após a revogação ou expiração do certificado de SCT, os procedimentos utilizados para confirmação da identidade do solicitante de novo certificado são os mesmos exigidos na solicitação inicial do certificado, na forma e prazo escritos nesta DPCT.

Após a expiração ou revogação de certificado de SCT, a ACT Certisign executa os processos regulares de geração de seu novo par de chaves, conforme descrito no item 6.1.1 desta DPCT.

4.6.2. A geração de um novo par de chaves e instalação do respectivo certificado no SCT deve ser realizada somente por funcionários com perfis qualificados, através de duplo controle, em ambiente físico seguro.

4.7. Comprometimento e Recuperação de Desastre

4.7.1. Disposições Gerais

4.7.1.1. A ACT Certisign possui um Plano de Continuidade de Negócios , estabelecido conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4], testado anualmente para garantir a continuidade de seus serviços críticos.

4.7.1.2 A ACT Certisign assegura, no caso de comprometimento de sua operação por qualquer um dos motivos relacionados nos itens abaixo, que as informações relevantes são disponibilizadas aos subscritores e às terceiras partes. A ACT Certisign disponibiliza a todos os subscritores e terceiras partes uma descrição do comprometimento ocorrido.

4.7.1.3 No caso de comprometimento de uma operação do SCT (por exemplo, comprometimento da chave privada do SCT), suspeita de comprometimento ou perda de calibração, o SCT não deverá emitir carimbo do tempo até que sejam tomadas medidas para recuperação do comprometimento.

4.7.1.4 Em caso de comprometimento grave da operação da ACT Certisign , sempre que possível, ela disponibiliza a todos os subscritores e terceiras partes informações que possam ser utilizadas para identificar os carimbos do tempo que podem ter sido afetados, a não ser que isso viole a privacidade dos subscritores ou comprometa a segurança dos serviços da ACT Certisign.

4.7.2. Recursos computacionais, software, e dados corrompidos

Em caso de suspeita de corrupção de dados, softwares e/ou recursos computacionais, o fato é comunicado ao Gerente de Segurança da ACT Certisign, que decreta o início da fase de resposta. Nessa fase, uma rigorosa inspeção é realizada para verificar a veracidade do fato e as consequências que o mesmo pode gerar. Esse procedimento é realizado por um grupo pré-determinado de funcionários devidamente treinados para essa situação. Caso haja necessidade, o Gerente de Segurança decretará a contingência.

4.7.3. Certificado do SCT é revogado

Em caso de revogação do certificado do SCT Certisign todos os carimbos do tempo subsequentes estarão automaticamente inválidos. O SCT será desabilitado no SGACT pelo Administrador. Não haverá recuperação do certificado do SCT no caso de revogação, é necessária a geração de um novo par de chaves e o Administrador precisará cadastrar o novo SCT.

4.7.4. Chave privada do SCT é comprometida

4.7.4.1. Em caso de suspeita de comprometimento de chave da ACT Certisign, o fato é imediatamente comunicado ao Gerente de Segurança que, juntamente com o Gerente de Criptografia da ACT Certisign, decretam o início da fase resposta e seguirão um plano de ação para analisar a veracidade e a dimensão do fato. Caso haja necessidade, será declarada a contingência e então as seguintes providências serão tomadas:

a) O certificado do SCT será revogado e todos os carimbos do tempo subsequentes considerados inválidos.

b) Cerimônias específicas serão realizadas para geração de novos pares de chaves. Isso não acontecerá se a ACT Certisign estiver encerrando suas atividades

4.7.5. Calibração e sincronismo do SCT são perdidos

O processo de sincronização do relógio interno dos equipamentos de SCT é realizado por meio do protocolo DS/NTP, que exige uma TAC (Time Atribbute Certificate) válida, enviada pelo ITI. Caso não exista uma TAC ou a TAC esteja expirada, o serviço de SCT não realiza nenhuma

assinatura de tempo até que um novo processo de sincronia seja realizado e uma TAC válida seja recebida.

4.7.6. Segurança dos recursos após desastre natural ou de outra natureza

Em caso de desastre natural ou de outra natureza, como por exemplo, incêndio ou inundação ou em caso de impossibilidade de acesso ao site, o Departamento de Infra-estrutura, responsável pela contingência, notifica o Gerente de Segurança e segue um procedimento que descreve detalhadamente os passos a serem seguidos para:

a) garantir a integridade física das pessoas que se encontram nas instalações da ACT Certisign;

b) monitorar e controlar o foco da contingência;

c) minimizar os danos aos ativos de processamento da companhia, de forma a evitar a descontinuidade dos serviços.

4.8. Extinção dos serviços de ACT ou PSS

4.8.1. Observado o disposto no item 4 do documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5], este item da DPCT deve descrever os requisitos e os procedimentos que deverão ser adotados nos casos de extinção dos serviços da ACT Certisign ou de um PSS a ela vinculado.

4.8.2. A ACT Certisign assegura que possíveis rompimentos com os subscritores e terceiras partes, em consequência da cessação dos serviços de carimbo do tempo da ACT Certisign são minimizados e, em particular, asseguram a manutenção continuada da informação necessária para verificar a precisão dos carimbos do tempo que emitiu.

4.8.3 Antes de a ACT Certisign cessar seus serviços de carimbo do tempo os seguintes procedimentos são executados, no mínimo:

a) a ACT Certisign disponibiliza a todos os subscritores e partes receptoras informações a respeito de sua extinção;

b) a ACT Certisign revoga a autorização de todos os PSSs e subcontratados que atuam em seu nome para a realização de quaisquer funções que se relacionam ao processo de emissão do carimbo do tempo;

c) a ACT Certisign transfere a outra ACT, após aprovação da AC-Raiz, as obrigações relativas à manutenção de arquivos de registro e de auditoria necessários para demonstrar a operação correta da ACT, por um período razoável;

d) a ACT Certisign mantém ou transfere a outra ACT, após aprovação da AC-Raiz, suas obrigações relativas a disponibilidade sua chave pública ou seus certificados a terceiras partes, por um período razoável;

e) as chaves privadas dos SCT serão destruídas de forma que não possam ser recuperadas;

f) a ACT Certisign solicita a revogação dos certificados de seus SCT;

g) A ACT Certisign notifica todas as entidades afetadas.

4.8.4. A ACT Certisign providencia os meios para cobrir os custos de cumprimento destes requisitos mínimos no caso de falência ou se por outros motivos se ver incapaz de arcar com os seus custos.

5. CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Nos itens seguintes são descritos os controles de segurança implementados pela ACT responsável pela DPCT e pelos PSSs a ela vinculados para executar de modo seguro suas funções.

5.1. Segurança Física

Nos itens seguintes desta DPCT são descritos os controles físicos referentes às instalações que abrigam os sistemas da ACT responsável e das PSS vinculadas.

5.1.1. Construção e localização das instalações de ACT

5.1.1.1. A localização e o sistema de carimbo de tempo da ACT Certisign não são publicamente identificados. Não há identificação pública externa das instalações e, internamente, não existem ambientes compartilhados que permitam visibilidade das operações de emissão de carimbos do tempo. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.2. Acesso físico nas instalações de ACT

A ACT Certisign implementa um sistema de controle de acesso físico que garante a segurança de suas instalações, conforme a POLÍTICA DE SEGURANÇA DA ICPBRASIL [4] e os requisitos que seguem.

5.1.2.1. Níveis de Acesso

5.1.2.1.1. A ACT Certisign possui 4 (quatro) níveis de acesso físico aos diversos ambientes e mais 1 (um) níveis de proteção da chave privada da ACT Certisign;

5.1.2.1.2. O primeiro nível – ou nível 1 – situa-se após a primeira barreira de acesso às instalações da ACT Certisign. Para entrar em uma área de nível 1, cada indivíduo é identificado e registrado por segurança armada. A partir desse nível, pessoas estranhas à operação da ACT Certisign transitam devidamente identificadas e acompanhadas.

Nenhum tipo de processo operacional ou administrativo da ACT Certisign é executado nesse nível.

5.1.2.1.3. Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações da ACT Certisign em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, têm sua entrada controlada e somente são utilizados mediante autorização formal e supervisão.

5.1.2.1.4. O segundo nível – ou nível 2 – é interno ao primeiro e requer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da

ACT Certisign. A passagem do primeiro para o segundo nível exige identificação por meio eletrônico e o uso de crachá.

5.1.2.1.5. O terceiro nível – ou nível 3 – situa-se dentro do segundo, sendo o primeiro nível a abrigar material e atividades sensíveis da operação da ACT Certisign.

Qualquer atividade relativa ao ciclo de vida dos carimbos do tempo é executada a partir desse nível.

Pessoas não envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não possuem permissão de acesso não permanecem nesse nível se não estiverem acompanhadas por alguém que tenha essa permissão.

5.1.2.1.6. No terceiro nível são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle são requeridos para a entrada nesse nível: identificação individual, por meio de cartão eletrônico, e identificação biométrica.

5.1.2.1.7. Telefones celulares, bem como outros equipamentos portáteis de comunicação, exceto aqueles exigidos para a operação da ACT Certisign, não são admitidos a partir do nível 3.

5.1.2.1.8. No quarto nível (nível 4), interior ao terceiro, é onde ocorrem atividades especialmente sensíveis da operação da ACT Certisign tais como emissão de carimbos do tempo, emissão de LCR e a disponibilidade à resposta a consulta OCSP. Todos os sistemas e equipamentos necessários a estas atividades estão localizados a partir desse nível. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, é exigido, em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas é exigida enquanto o ambiente estiver sendo ocupado.

5.1.2.1.9. No quarto nível, todas as paredes, piso e teto são revestidos de aço e concreto. As paredes, piso e o teto, são inteiriços, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gazes e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não permitem a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 – que constituem as chamadas salas-cofre - possuem proteção contra interferência eletromagnética externa.

5.1.2.1.10. As salas-cofre foram construídas segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas foram sanadas por normas internacionais pertinentes.

5.1.2.1.11. Na ACT Certisign, existem ambientes de quarto nível para abrigar e segregar:

a) equipamentos de produção on-line, gabinete reforçado de armazenamento e equipamentos de rede e infra-estrutura - firewall, roteadores, switches e servidores - (Data Center);

b) equipamentos de produção off-line e cofre de armazenamento (Sala de cerimônia);

5.1.2.1.12. O quinto nível (nível 5), interior aos ambientes de nível 4, compreende um cofre interior à sala de cerimônia e um gabinete reforçado trancado no Data Center. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos são armazenados em ambiente de nível 5 ou superior.

5.1.2.1.13. Existem na ACT Certisign ambientes de níveis 3 (três) e 4 (quatro) para abrigar e segregar, quando for o caso:

a) equipamentos de produção e cofre de armazenamento; e

b) equipamentos de rede e infra-estrutura (firewall, roteadores, switches e servidores).

5.1.2.1.14. O sexto nível (nível 6) constitui-se de pequenos depósitos localizados no interior do cofre da sala de cerimônia (Nível 5). Cada um desses depósitos dispõe de 2 fechaduras, sendo uma individual e a outra comum a todos os depósitos. Os dados de ativação da chave privada da ACT Certisign são armazenados nesses depósitos.

5.1.2.1.15. O quarto nível, ou nível 4, interior ao ambiente de nível 3, deverá compreender pelo menos 2 cofres ou gabinetes reforçados trancados, que abrigarão, separadamente:

a) os SCT e equipamentos criptográficos;

b) outros materiais criptográficos, tais como cartões, chaves, dados de ativação e suas cópias.

5.1.2.1.16. Para garantir a segurança do material armazenado, os cofres ou os gabinetes deverão obedecer às seguintes especificações mínimas:

a) ser feitos em aço ou material de resistência equivalente; e

b) possuir tranca com chave.

5.1.2.1.17. O cofre ou gabinete que abrigará os SCTs deverá ser trancado de forma que sua abertura seja possível somente com a presença de dois funcionários de confiança da ACT Certisign.

5.1.2.2. Sistemas Físicos de Detecção

5.1.2.2.1. Todas as passagens entre os níveis de acesso, bem como as salas de operação de nível 4, são monitoradas por câmeras de vídeo ligadas a um sistema de gravação 24x7.

5.1.2.2.2. Os DVDs resultantes da gravação 24x7 são armazenados por um ano. Eles são testados (verificação de trechos aleatórios no início, meio e final da fita) trimestralmente, com a escolha de, no mínimo, um DVD referente a cada semana. Esses DVDs são armazenados em ambiente de terceiro nível.

5.1.2.2.3. Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes. A partir do nível 2, vidros que separam os níveis de acesso, possuem alarmes de quebra de vidros ligados ininterruptamente.

5.1.2.2.4. As mídias resultantes dessa gravação deverão ser armazenadas por, no mínimo, 1 (um) ano, em ambiente de nível 6.

5.1.2.2.5. O sistema de notificação de alarmes utiliza 2 (dois) meios de notificação: sonoro e visual.

5.1.2.3. Sistema de controle de acesso

O sistema de controle de acesso está baseado em um ambiente de nível 4.

5.1.3. Energia e ar condicionado nas instalações da ACT Certisign

5.1.3.1. A infra-estrutura do ambiente de certificação da ACT Certisign está dimensionada com sistemas e dispositivos que garantem o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia são mantidas de forma a atender os requisitos de disponibilidade dos sistemas da ACT Certisign e seus respectivos serviços. Um sistema de aterramento está disponível no ambiente da ACT Certisign.

5.1.3.2. Todos os cabos elétricos são protegidos por tubulações ou dutos apropriados.

5.1.3.3. Existem tubulações, dutos, calhas, quadros e caixas – de passagem, distribuição e terminação – projetados e construídos de forma a facilitar vistorias e a detecção de tentativas de violação. São utilizados dutos separados para os cabos de energia, telefonia e dados.

5.1.3.4. Todos os cabos são catalogados, identificados e periodicamente vistoriados, a cada 6 meses, na busca de evidências de violação ou de outras anormalidades.

5.1.3.5. São mantidos atualizados os registros sobre a topologia da rede de cabos, observados os requisitos de sigilo estabelecidos pela Política de Segurança da ICP-Brasil. Qualquer modificação nessa rede é previamente documentada.

5.1.3.6. Não são admitidas instalações provisórias, fiações expostas ou diretamente conectadas às tomadas sem a utilização de conectores adequados.

5.1.3.7. O sistema de climatização atende os requisitos de temperatura e umidade exigidos pelos equipamentos utilizados no ambiente e dispõe de filtros de poeira. Nos ambientes de nível 4, o sistema de climatização é independente e tolerante à falhas.

5.1.3.8. A temperatura dos ambientes atendidos pelo sistema de climatização é permanentemente monitorada pelo sistema de notificação de alarmes.

5.1.3.9 A capacidade de redundância de toda a estrutura de energia e ar condicionado do ambiente de nível 3 da ACT Certisign deverá ser garantida por meio de nobreaks e geradores de porte compatível.

5.1.4. Exposição à água nas instalações de ACT Certisign

A estrutura inteiriça do ambiente de nível 4 construído na forma de célula estanque, provê proteção física contra exposição à água e infiltrações provenientes de qualquer fonte externa.

5.1.5. Prevenção e proteção contra incêndio nas instalações da ACT Certisign

5.1.5.1. Nas instalações da ACT Certisign não é permitido fumar ou portar objetos que produzam fogo ou faísca, a partir do ambiente de nível 2.

5.1.5.2. Existem, a partir do ambiente de nível 3, extintores de incêndio das classes B e C, para apagar incêndios em combustíveis e equipamentos elétricos, dispostos no ambiente de forma a facilitar o seu acesso e manuseio.

Os sistemas de prevenção contra incêndios, internos aos ambientes, possibilitam alarmes preventivos antes de fumaça visível, disparados somente com a presença de partículas que caracterizam o sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

5.1.5.3. Existe, a partir do ambiente de nível 3, sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso à sala-cofre constituem eclusas, onde uma porta só abre quando a anterior estiver fechada.

5.1.5.4. Nos ambientes de nível 1 e 2 da ACT Certisign, existem extintores de incêndio para todas as classes de fogo, dispostos em locais que facilitam o seu acesso e manuseio.

Em caso de incêndio nas instalações da ACT Certisign, a temperatura interna da sala-cofre de nível 4 não excede 50 graus Celsius, e a sala suporta esta condição por, no mínimo, uma hora.

5.1.5.5 Mecanismos específicos são implantados pela ACT Certisign para garantir a segurança de seu pessoal e de seus equipamentos em situações de emergência. Esses mecanismos permitem o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos aciona imediatamente os alarmes de abertura de portas.

5.1.6. Armazenamento de mídia nas instalações de ACT Certisign

A ACT Certisign atende às normas NBR 11.515 e NB 1334 ("Critérios de Segurança Física Relativos ao Armazenamento de Dados").

5.1.7. Destruição de lixo nas instalações da ACT

5.1.7.1. Todos os documentos em papel que contenham informações classificadas como sensíveis são triturados antes de ir para o lixo.

5.1.7.2. Todos os dispositivos magnéticos não mais utilizáveis e que tenham sido anteriormente utilizados para o armazenamento de informações sensíveis são desmagnetizados com ferramentas específicas, e são fisicamente destruídos.

5.1.8. Sala externa de arquivos (off-site) para ACT

Uma sala de armazenamento externa à instalação técnica principal da ACT Certisign é usada para o armazenamento e retenção de cópia de segurança de dados. Essa sala esta disponível ao pessoal autorizado 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e atende aos requisitos mínimos estabelecidos por este documento para um ambiente de nível 2.

5.2. Controles Procedimentais

Nos itens seguintes da DPCT são descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados na ACT Certisign e nos PSSs a ela vinculados, juntamente com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, é estabelecido o número de pessoas requerido para sua execução.

5.2.1. Perfis qualificados

5.2.1.1. A ACT Certisign pratica uma política de segregação de funções, controlando e registrando o acesso físico e lógico às funções críticas do ciclo de vida da operação da ACT, de forma a garantir a segurança da atividade de carimbo de tempo e evitar a manipulação desautorizada do sistema. As ações permitidas são limitadas de acordo com o perfil de cada cargo.

5.2.1.2. A ACT Certisign estabelece 4 perfis distintos para sua operação, atribuídos às seguintes gerências:

a) Administrador do sistema - autorizado a instalar, configurar e manter os sistemas confiáveis para gerenciamento do carimbo do tempo, bem como administrar a implementação das práticas de segurança da ACT. Autorizado a realizar backup e recuperação do sistema;

b) Operador de sistema - responsável pela operação diária dos sistemas confiáveis da ACT. Pode configurar novos usuários (subscritores) autorizados a solicitar carimbos de tempos e seus limites de utilização.

c) Auditor de Sistema - autorizado a ver arquivos e auditar os logs dos sistemas confiáveis da ACT

d) Cliente/subscritor – realiza operações de solicitação de carimbos de tempo e acesso a relatório consolidado de consumo (bilhetagem).

5.2.1.3. Os operadores do sistema de carimbo do tempo da ACT Certisign recebem treinamento específico antes de obter qualquer tipo de acesso ao sistema. O tipo e o nível de acesso estão determinados, em documento formal (Política de Segurança da ACT Certisign), com base nas necessidades de cada perfil.

5.2.1.4. A ACT Certisign possui rotinas de atualização das permissões de acesso e procedimentos específicos para situações de demissão ou mudança de função dos empregados. Existe uma lista de revogação com todos os recursos, antes disponibilizados, que o empregado devolve à ACT Certisign no ato de seu desligamento.

5.2.2. Número de pessoas necessário por tarefa

5.2.2.1. É implementado controle multiusuário para a geração e a utilização da chave privada dos SCT operados pela ACT Certisign, conforme o descrito em 6.1.1.

5.2.2.2. Todas as tarefas executadas no ambiente onde esta localizado o equipamento de certificação da ACT Certisign requerem a presença de, no mínimo, 2 (dois) de seus empregados com perfis qualificados. As demais tarefas da ACT podem ser executadas por um único empregado.

5.2.3. Identificação e autenticação para cada perfil

5.2.3.1 A DPCT garante que todo empregado da ACT Certisign tem sua identidade e perfil verificados antes de:

a) ser incluído em uma lista de acesso físico às instalações da ACT;

b) ser incluído em uma lista para acesso lógico aos sistemas confiáveis da ACT;

c) ser incluído em uma lista para acesso lógico aos SCTs da ACT.

5.2.3.2. Os certificados, contas e senhas utilizados para identificação e autenticação dos empregados:

a) são diretamente atribuídos a um único empregado;

b) não são compartilhados; e

c) são restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.3. A ACT Certisign adota padrão de utilização de "senhas fortes", definido na sua Política de Segurança e em conformidade com a Política de Segurança da ICP-Brasil, juntamente com procedimentos de validação dessas senhas.

5.3. Controles de Pessoal

Nos itens seguintes desta DPCT são descritos requisitos e procedimentos, implementados pela ACT Certisign e PSS vinculados em relação a todo o seu pessoal, referentes a aspectos como: verificação de antecedentes e de idoneidade, treinamento e reciclagem profissional, rotatividade de cargos,

sanções por ações não autorizadas, controles para contratação e documentação a ser fornecida. Esta DPCT garante que todos os empregados da ACT Certisign e PSS vinculados, encarregados de tarefas operacionais têm registrado em contrato ou termo de responsabilidade:

a) os termos e as condições do perfil que ocuparão;

b) o compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil; e

c) o compromisso de não divulgar informações sigilosas a que tenham acesso.

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal da ACT Certisign e dos PSSs vinculados envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição e gerenciamento de carimbos do tempo é admitido conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

5.3.2. Procedimentos de verificação de antecedentes

5.3.2.1. Com o propósito de resguardar a segurança e a credibilidade das entidades, todo o pessoal da ACT Certisign e dos PSSs vinculados envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição e gerenciamento de carimbos do tempo é submetido, pelo menos, a:

a) verificação de antecedentes criminais;

b) verificação de situação de crédito;

c) verificação de histórico de empregos anteriores; e

d) comprovação de escolaridade e de residência.

5.3.3. Requisitos de treinamento

Todo o pessoal da ACT Certisign e dos PSSs vinculados envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição e gerenciamento de carimbos do tempo recebe treinamento documentado, suficiente para o domínio dos seguintes temas:

a) princípios e tecnologias de carimbo do tempo e sistema de carimbos do tempo em uso na ACT;

b) ICP-Brasil;

c) princípios e tecnologias de certificação digital e de assinaturas eletrônicas;

d) princípios e mecanismos de segurança de redes e segurança da ACT;

e) procedimentos de recuperação de desastres e de continuidade do negócio;

f) familiaridade com procedimentos de segurança, para pessoas com responsabilidade de Oficial de Segurança;

g) familiaridade com procedimentos de auditorias em sistemas de informática, para pessoas com responsabilidade de Auditores de Sistema;

h) outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4. Frequência e requisitos para reciclagem técnica

O pessoal da ACT Certisign e dos PSSs vinculados envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição e gerenciamento de carimbo de tempo é mantido atualizado sobre mudanças tecnológicas nos sistemas da ACT Certisign.

5.3.5. Frequência e sequência de rodízio de cargos

Não estabelecido.

5.3.6. Sanções para ações não autorizadas

5.3.6.1. Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da ACT Certisign ou de um PSS vinculado, o acesso dessa pessoa ao sistema de certificação é suspenso, é instaurado processo administrativo para apurar os fatos e, se for o caso, são tomadas as medidas administrativas e legais cabíveis.

5.3.6.2. O processo administrativo referido acima contém, no mínimo, os seguintes itens:

a) relato da ocorrência com "modus operandis";

b) identificação dos envolvidos;

c) eventuais prejuízos causados;

d) punições aplicadas, se for o caso; e

e) conclusões.

5.3.6.3. Concluído o processo administrativo, a ACT Certisign encaminha suas conclusões à AC Raiz.

5.3.6.4. As punições passíveis de aplicação, em decorrência de processo administrativo, são:

a) advertência;

b) suspensão por prazo determinado; ou

c) impedimento definitivo de exercer funções no âmbito da ICP-Brasil.

5.3.7. Requisitos para contratação de pessoal

Todo o pessoal da ACT Certisign e dos PSSs vinculados envolvido em atividades diretamente relacionadas com os processos de emissão, expedição e gerenciamento de carimbos de tempo é contratado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

5.3.8. Documentação fornecida ao pessoal

5.3.8.1. A ACT Certisign disponibiliza para todo o seu pessoal e para o pessoal dos PSSs vinculados:

a) sua DPCT;

b) as PCTs que implementa;

c) a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4];

d) a PS DA ACT Certisign;

e) documentação operacional relativa a suas atividades; e

f) contratos, normas e políticas relevantes para suas atividades.

5.3.8.2. A documentação fornecida é classificada segundo a política de classificação de informação definida pela ACT Certisign e é mantida atualizada.

6. CONTROLES TÉCNICOS DE SEGURANÇA

Nos itens seguintes, esta DPCT define as medidas de segurança implantadas pela ACT Certisign para proteger suas chaves criptográficas e manter o sincronismo de seus SCTs. Também são definidos outros controles técnicos de segurança utilizados pela ACT Certisign e pelos PSSs vinculados na execução de suas funções operacionais.

6.1. Ciclo de Vida da Chave Privada do SCT

O SCT permite:

a) geração do par de chaves criptográficas;

b) geração de requisição de certificado digital;

c) exclusão de requisição de certificado digital;

d) instalação de certificados digitais;

e) renovação de certificado digital (com a geração de novo par de chaves);

f) proteção de chaves privadas.

6.1.1. Geração do par de chaves

6.1.1.1. O par de chaves criptográficas da ACT Certisign é gerado pela própria ACT Certisign, após ter sido credenciada e autorizada a funcionar no âmbito da ICP-Brasil.

6.1.1.2. A ACT Certisign assegura que quaisquer chaves criptográficas são geradas em circunstâncias controladas. Em particular:

a) geração da chave de assinatura do SCT é realizada em um ambiente físico seguro, por pessoal em funções de confiança sob, pelo menos, controle duplo. O pessoal autorizado para realizar essa função será limitado àqueles que receberam essa responsabilidade de acordo com as práticas da ACT Certisign;

b) a geração da chave de assinatura do SCT será realizada dentro de módulo criptográfico que cumpra os requisitos dispostos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [10];

c) o algoritmo de geração de chave do SCT, o comprimento da chave assinante resultante e o algoritmo de assinatura usado para assinar o carimbo do tempo constam no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS NA ICP-BRASIL [10].

6.1.1.3. A ACT Certisign garante que as chaves privadas são geradas de forma a não serem exportáveis.

6.1.2. Geração de Requisição de Certificado Digital

O SCT possui mecanismo para geração de requisição de certificado digital correspondente à chave privada gerada no módulo criptográfico interno ao SCT, que atende ao formato definido pela ICP-Brasil.

6.1.3. Exclusão de Requisição de Certificado Digital

O SCT deve garante que a exclusão de uma requisição de certificado digital, por desistência de emissão do certificado, obrigatoriamente implicará a exclusão da chave privada correspondente.

6.1.4. Instalação de Certificado Digital

6.1.4.1. A geração do par de chaves / requisição de certificado (PKCS#10) assim como a instalação do certificado digital é realizada por um Administrador autorizado, por meio da interface segura e controlada do SCT. São informados, além do certificado digital, os certificados intermediários e o certificado raiz do caminho de certificação do certificado gerado.

6.1.4.2. O SCT realiza no mínimo a conferência dos itens descritos a seguir antes da instalação do certificado:

a) verifica se chave privada correspondente a esse certificado encontra-se em seu módulo criptográfico interno;

b) verifica se o certificado possui as extensões obrigatórias;

c) valida o caminho de certificação.

6.1.5. Renovação de Certificado Digital

O SCT permite a renovação do certificado digital, através da geração de requisição de certificado digital, gerada através de novo par de chaves que deve manter as mesmas informações do certificado a ser renovado.

As informações contidas nos certificados são inseridas pelo administrador do sistema.

A geração do par de chaves / requisição de certificado (PKCS#10) assim como a instalação do certificado digital é realizada por um Administrador autorizado, por meio da interface segura e controlada do SCT.

6.1.6. Disponibilização de chave pública da ACT Certisign para usuários

A ACT Certisign disponibiliza o seu certificado e todos os certificados da cadeia de certificação para os usuários da ICP-Brasil, através endereço Web: http://icp-brasil.certisign.com.br/repositorio/act-certisign/index.htm.

6.1.7. Tamanhos de chave

Cada PCT implementada pela ACT Certisign define o tamanho das chaves criptográficas associadas aos certificados emitidos, com base nos requisitos aplicáveis estabelecidos pelo documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

O tamanho das chaves criptográficas associadas ao certificado da ACT Certisign é de 2048 bits.

6.1.8. Geração de parâmetros de chaves assimétricas

A geração dos parâmetros de chaves assimétricas é gerada em módulo de segurança criptográfico, utilizando os padrões de segurança FIPS 140-2 nível 3, e adotarão o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

6.1.9. Verificação da qualidade dos parâmetros

Os parâmetros para geração das chaves são baseados nos padrões de segurança FIPS 140-2 nível 3, e são aplicados de acordo com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

6.1.10. Geração de chave por hardware ou software

As chaves da ACT Certisign são geradas, armazenadas e utilizadas dentro de hardware específico, compatíveis com as normas estabelecidas pelo padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

6.1.11. Propósito de uso de chave

As chaves privadas dos SCT operados pela ACT Certisign somente serão utilizadas para assinatura dos carimbos do tempo por ela emitidos, de acordo com as normas estabelecidas pelo padrão definido no documento em conformidade com o documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL [2].

6.2. Proteção da Chave Privada

Nos itens seguintes, a DPCT estabelece os procedimentos de segurança que adotará para a proteção da chave privada de seus SCTs.

6.2.1. Padrões para módulo criptográfico

O módulo criptográfico de geração de chaves assimétricas da ACT Certisign adota o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

Os Titulares de Certificado devem garantir que o módulo criptográfico utilizado na geração e utilização de suas chaves criptográficas segue o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

6.2.2. Controle "n de m" para chave privada

Não se aplica.

6.2.3. Recuperação de chave privada

Não é permitido, no âmbito da ICP-Brasil, a recuperação de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

6.2.4. Cópia de segurança (backup) de chave privada

Não é permitido, no Âmbito da ICP-Brasil, a geração de cópia de segurança (backup) de chaves privadas de assinatura digital de SCT.

6.2.5. Arquivamento de chave privada

A ACT Certisign não arquiva chaves privadas de assinatura digital de seus SCT, entendendo-se como arquivamento o armazenamento da chave privada. O equipamento de SCT exige que os certificados instalados no mesmo possuam a identificação de número de série do equipamento, sendo assim, em caso de pane/perda total, um novo certificado digital deve ser instalado no equipamento de reposição.

6.2.6. Inserção de chave privada em módulo criptográfica

Não se aplica.

6.2.7. Método de ativação de chave privada

A ativação das chaves privadas do SCT é coordenada pelo seu Gerente de Criptografia, onde 3 de um grupo de 5 funcionários com perfis qualificados da ACT Certisign, detentores de partição da chave de ativação do equipamento criptográfico (PIN), apresentam tais componentes em cerimônia específica.

Esses funcionários são identificados pelo crachá funcional emitido pela ACT Certisign contendo fotografia, nome, e departamento do funcionário.

6.2.8. Método de desativação de chave privada

A chave privativa da ACT Certisign, instalada em ambiente de produção dos sistemas de certificação, localiza-se em nível de segurança 4, onde só é permitido o acesso ao ambiente em duplas devidamente autorizadas pelo sistema de controle de acesso da ACT Certisign.

Dentro deste ambiente, somente funcionários qualificados do departamento de operações têm acesso ao sistema de certificação de produção, onde são executados os comandos de desativação do sistema, após a sua devida identificação e autorização feita através de mecanismos nativos do sistema operacional.

Esses funcionários são identificados pelo crachá funcional emitido pela ACT Certisign contendo fotografia, nome, e departamento do funcionário.

Cada PCT implementada descreve os requisitos e os procedimentos necessários para a desativação da chave privada de entidade titular de certificado.

6.2.9. Método de destruição de chave privada

O Gerente de Criptografia da ACT Certisign, de posse da chave privada original a ser destruída, acompanhado do Gerente de Segurança e do representante legal da ACT Certisign, titular do certificado, conduz cerimônia especifica, em ambiente de nível 4 de segurança, para reinicialização das mídias de armazenamento das chaves privadas, não deixando informações remanescente sensíveis nessas mídias.

Os Gerentes de Criptografia e Segurança são identificados pelo crachá funcional emitido pela ACT Certisign contendo fotografia, nome, e departamento do funcionário. O representante legal da ACT Certisign é identificado através de cédula de identidade ou passaporte, se estrangeiro.

Cada PCT implementada descreve os requisitos e os procedimentos necessários para a destruição da chave privada de entidade titular de certificado.

6.3. Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1. Arquivamento de chave pública

As chaves públicas dos SCT da ACT Certisign, após a expiração dos certificados correspondentes, serão guardadas pela AC que emitiu os certificados, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

6.3.2. Períodos de uso para as chaves pública e privada

6.3.2.1. As chaves privadas dos SCTs da ACT Certisign pela DPCT deverão ser utilizadas apenas durante o período de validade dos certificados correspondentes. As correspondentes chaves públicas poderão ser utilizadas durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos respectivos certificados.

6.3.2.2. O sistema de geração de carimbos do tempo deverá rejeitar qualquer tentativa de emitir carimbos do tempo caso sua chave privada de assinatura esteja vencida ou revogada.

6.4. Dados de Ativação da Chave do SCT

6.4.1. Proteção dos dados de ativação

Não se aplica.

6.4.2. Outros aspectos dos dados de ativação

Não se aplica.

6.5. Características do SCT

6.5.1. O Servidor de Carimbo do tempo é um sistema de hardware e software que executa a geração de carimbos do tempo, atendendo às especificações descritas nesta seção. A responsabilidade pelo atendimento é do fabricante do SCT.

6.5.2. O SCT mantém o relógio interno do HSM sincronizado com a fonte confiável de tempo (FCT) mantida pela AC-Raiz. A avaliação da manutenção desse sincronismo é realizada pela Entidade Auditora do Tempo (EAT).

O processo de sincronização do relógio interno dos equipamentos de SCT é realizado por meio do protocolo DS/NTP, que exige uma TAC (Time Atribbute Certificate) válida, enviada pelo ITI. Caso não exista uma TAC ou a TAC esteja expirada, o serviço de SCT não realiza nenhuma assinatura de tempo até que um novo processo de sincronia seja realizado e uma TAC válida seja recebida.

6.5.3. O SCT garante que a emissão dos carimbos do tempo seja feita em conformidade com o tempo constante do relógio interno do HSM e que a assinatura digital do carimbo do tempo seja feita dentro do HSM.

6.5.4. Neste item da DPCT, são definidas as características dos SCTs utilizados pela ACT Certisign. O SCT possui como características mínimas:

a) emitir os carimbos do tempo na mesma ordem em que são recebidas as requisições;

b) permitir gerenciamento e proteção de chaves privadas;

c) utilizar certificado digital válido emitido por AC credenciada pelo Comitê Gestor da ICP-Brasil; autoridade de carimbo do tempo;

d) permitir identificação e registro de todas as ações executadas e dos carimbos do tempo emitidos;

e) permitir que o relógio interno de seu HSM se mantenha sincronizado com a FCT;

f) garantir a irretroatividade na emissão de carimbos do tempo;

g) prover meios para que a EAT possa auditar e sincronizar o relógio interno do seu HSM;

h) garantir que o acesso da EAT seja realizado através de autenticação mútua entre o SCT e o SAS, utilizando certificados digitais;

i) possuir certificado de especificações emitido pelo fabricante;

j) somente emitir carimbo do tempo se:

i. possuir alvará vigente emitido pela EAT, a fim de garantir que a precisão do sincronismo do relógio do seu HSM esteja de acordo com o relógio da FCT;

ii. possuir certificado digital dentro do período de validade e não revogado, emitido por AC credenciada na ICP-Brasil;

iii. possuir certificado de especificações emitido e assinado pelo fabricante do SCT.

6.6. Ciclo de Vida de Módulo Criptográfico

A instalação e a ativação do SCT são realizadas sempre com a presença de no mínimo duas pessoas formalmente designadas para a tarefa em ambiente seguro e controlado. Para a geração de chaves é necessária a autenticação com certificado digital para acessar a interface administrativa.

Para manutenção, ativação e inicialização do MSC é necessária a ativação mínima das dos cartões de segurança do equipamento (3 dos 5 responsáveis designados).

6.7. Auditoria e Sincronização de Relógio de SCT

A ACT Certisign certificar-se que seus SCTs estejam sincronizados com o UTC dentro da precisão declarada nas PCTs respectivas e, particularmente, que:

a) os valores de tempo utilizados pelo SCT na emissão de carimbos do tempo sejam rastreáveis até a hora UTC;

b) a calibração dos relógios dos SCTs seja mantida de tal forma que não se afaste da precisão declarada na PCT;

c) os relógios dos SCTs estejam protegidos contra ataques, incluindo violações e imprecisões causadas por sinais elétricos ou sinais de rádio, evitando que sejam descalibrados e permitindo que qualquer modificação possa ser detectada;

d) a ocorrência de perda de sincronização do valor do tempo indicado em um carimbo do tempo com o UTC seja detectada pelos controles do sistema;

e) o SCT deixe de emitir carimbos do tempo, caso receba da EAT alvará com validade igual a zero, situação que ocorrerá se a EAT constatar que o relógio do SCT está fora da precisão estabelecida na PCT correspondente;

f) a sincronização dos relógios dos SCTs seja mantida mesmo quando ocorrer a inserção de um segundo de transição (leap second);

g) a EAT tenha acesso com perfil de auditoria aos logs resultantes das ASRs.

6.8. Controle de Segurança Computacional

6.8.1. Disposições Gerais

Esta DPCT indica os mecanismos utilizados para prover a segurança de suas estações de trabalho, servidores e demais sistemas e equipamentos, observado o disposto no item 9.3 da POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

6.8.2. Requisitos técnicos específicos de segurança computacional

6.8.2.1. A DPCT prevê que os SCTs e os equipamentos da ACT Certisign, usados nos processos de emissão, expedição, distribuição ou gerenciamento de carimbos do tempo implementa as seguintes características:

a) controle de acesso aos serviços e perfis da ACT;

b) clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da ACT;

c) uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;

d) geração e armazenamento de registros de auditoria da ACT;

e) mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e

f) mecanismos para cópias de segurança (backup).

6.8.2.2. Os requisitos de segurança computacional, utilizados para prover a segurança de suas estações de trabalho, servidores e demais sistemas e equipamentos, são implementados pelo sistema operacional ou por meio da combinação deste com o sistema de gerenciamento do carimbo do tempo e com mecanismos de segurança física.

6.8.2.3. Qualquer equipamento, ou parte desse, ao ser enviado para manutenção deverá ter apagadas as informações sensíveis nele contidas e controlados seu número de série e as datas de envio e de recebimento. Ao retornar às instalações da ACT Certisign, o equipamento que passou por manutenção deverá ser inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, deverão ser destruídas de maneira definitiva todas as

informações sensíveis armazenadas, relativas à atividade da ACT Certisign. Todos esses eventos deverão ser registrados para fins de auditoria.

6.8.2.4. Qualquer equipamento incorporado à ACT Certisign deverá ser preparado e configurado como previsto na PS implementada ou em outro documento aplicável, de forma a apresentar o nível de segurança necessário à sua finalidade.

6.8.3. Classificação da segurança computacional

A segurança computacional da ACT Certisign segue as recomendações Common Criteria.

6.9. Controles Técnicos do Ciclo de Vida

Nos itens seguintes desta DPCT são descritos, quando aplicáveis, os controles implementados pela ACT Certisign e pelos PSSs a ela vinculados no desenvolvimento de sistemas e no gerenciamento de segurança.

6.9.1. Controles de desenvolvimento de sistema

6.9.1.1. A ACT Certisign utiliza um modelo clássico espiral no desenvolvimento dos sistemas. São realizadas as fases de requisitos, análise, projeto, codificação e teste para cada interação do sistema utilizando tecnologias de orientação a objetos. Como suporte a esse modelo, a ACT Certisign utiliza uma gerência de configuração, gerência de mudança, testes formais e outros processos informais.

6.9.1.2. Os processos de projeto e desenvolvimento conduzidos pela ACT Certisign provêem documentação suficiente para suportar avaliações externas de segurança dos componentes da ACT Certisign.

6.9.2. Controles de gerenciamento de segurança

6.9.2.1. A ACT Certisign e seus PSS vinculados verificam os níveis configurados de segurança com periodicidade semanal e através de ferramentas do próprio sistema operacional. As verificações são feitas através da emissão de comandos de sistema e comparando-se com as configurações aprovadas. Em caso de divergência, são tomadas as medidas para recuperação da situação, conforme a natureza do problema e averiguação do fato gerador do problema para evitar sua recorrência.

6.9.2.2. A ACT Certisign e seus PSS vinculados utilizam metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema.

6.9.3. Classificações de segurança de ciclo de vida

Não se aplica.

6.10. Controles de Segurança de Rede

6.10.1. Diretrizes Gerais

6.10.1.1. Neste item são descritos os controles relativos à segurança da rede da ACT Certisign, incluindo firewalls e recursos similares, observado o disposto no item 9.3.3 da POLÍTICA DE SEGURANÇA DA ICP-BRASIL [4].

6.10.1.2. Todos os servidores e elementos de infra-estrutura e proteção de rede, tais como roteadores, hubs, switches, firewalls, e sistemas de detecção de intrusos (IDS), localizados no segmento de rede que hospeda o sistema de certificação estão localizados e operam em ambiente de nível 4.

6.10.1.3. As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções (patches), disponibilizadas pelos respectivos fabricantes são implantadas imediatamente após testes em ambiente de desenvolvimento ou homologação.

6.10.1.4. O acesso lógico aos elementos de infra-estrutura e proteção de rede é restrito, por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas implementam filtros de pacotes de dados, que permitem somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

6.10.1.5. O acesso à Internet é provido por no mínimo duas linhas de comunicação de sistemas autônomos (AS) distintos.

6.10.1.6. O acesso via rede aos SCTs e sistema de gestão da ACT CERTISIGN é permitido somente para os seguintes serviços:

a) pela EAT da ICP-Brasil, para o sincronismo e auditoria de relógios dos SCTs;

b) pela ACT, para a administração dos SCTs e sistemas de gestão a partir de equipamento conectado por rede interna ou por VPN estabelecida mediante endereçamento IP fixo previamente cadastrado junto à EAT;

c) pelo PSS da ACT, para a administração dos SCTs e sistemas de gestão a partir de equipamento conectado por rede interna ou por VPN estabelecida mediante endereçamento IP fixo previamente cadastrado junto à EAT;

d) pelo subscritor, para a solicitação e recebimento de carimbos do tempo.

6.10.2. Firewall

6.10.2.1. Mecanismos de firewall são implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. O firewall promove o isolamento, em sub-redes específicas, dos equipamentos servidores com acesso externo – a conhecida "zona desmilitarizada" (DMZ) – em relação aos equipamentos com acesso exclusivamente interno à ACT Certisign.

6.10.2.2. O software de firewall, entre outras características, implementa registros de auditoria.

6.10.2.3. O Oficial de Segurança deve verifica periodicamente as regras dos firewalls, para assegurar-se que apenas o acesso aos serviços realmente necessários é permitido e que está bloqueado o acesso a portas desnecessárias ou não utilizadas.

6.10.3. Sistema de detecção de intrusão (IDS)

6.10.3.1. O sistema de detecção de intrusão está configurado para reconhecer ataques em tempo real e respondê-los automaticamente, com medidas tais como: enviar traps SNMP, executar programas definidos pela administração da rede, enviar e-mail aos administradores, enviar mensagens de alerta aos firewalls ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas ou ainda a reconfiguração dos firewalls.

6.10.3.2. O sistema de detecção de intrusão reconhece diferentes padrões de ataques, inclusive contra o próprio sistema, com atualização da sua base de reconhecimento.

6.10.3.3. O sistema de detecção de intrusão provê o registro dos eventos em logs, recuperáveis em arquivos do tipo texto, além de implementar uma gerência de configuração.

6.10.4. Registro de acessos não-autorizados à rede

As tentativas de acesso não-autorizado – em roteadores, firewalls ou IDS – são registradas em arquivos para posterior análise. A freqüência de exame dos arquivos de registro é diária e todas as ações tomadas em decorrência desse exame são documentadas.

6.10.5. Outros controles de segurança de rede

6.10.5.1 A ACT Certisign implementa serviço de proxy, restringindo o acesso, a partir de todas suas estações de trabalho, a serviços que possam comprometer a segurança do ambiente ACT Certisign.

6.10.5.2 As estações de trabalho e servidores devem estar dotadas de antivírus, antispyware de outras ferramentas de proteção contra ameaças provindas da rede a que estão ligadas.

6.10.5.3. Os relógios dos SCTs são protegidos contra ataques, incluindo violações e imprecisões causadas por sinais elétricos ou sinais de rádio, para evitar que sejam

descalibrados. Qualquer modificação ocorrida nestes relógios deverá ser registrada e detectada.

6.11. Controles de Engenharia do Módulo Criptográfico

O módulo criptográfico utilizado para armazenamento da chave privada da ACT Certisign está em conformidade com o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [10].

7. Perfis dos Carimbos de Tempo

7.1. Diretrizes Gerais

Nos seguintes itens desta DPCT estão descritos os aspectos dos carimbos do tempo emitidos pela ACT Certisign, bem como das requisições que lhes são enviadas.

7.2. Perfil do Carimbo do tempo

Todos os carimbos do tempo emitidos pela ACT Certisign estão em conformidade com o formato definido pelo Perfil de Carimbo do tempo constante da European Telecommunications Stardards Institute Technical Specification 101 861 (ETSI TS 101 861) e devem seguir as definições constantes da RFC 3161.

7.2.1. Requisitos para um cliente TSP

7.2.1.1. Perfil para o formato do pedido

a) Parâmetros a serem suportados: nenhuma extensão precisa estar presente.

b) Algoritmos a serem usados: SHA1, SHA256, SHA384 e SHA512.

7.2.1.2. Perfil do formato da resposta

a) Parâmetros a serem suportados:

i. o campo accuracy deve ser suportado e compreendido;

ii. mesmo quando inexistente ou configurado como FALSO, o campo ordering deve ser suportado;

iii. o campo nounce deve ser suportado e verificado com o valor constante da requisição correspondente para que a resposta seja corretamente validada;

iv. nenhuma extensão necessita ser tratada ou suportada.

b) Algoritmos a serem suportados: SHA1, SHA256, SHA384 e SHA512.

c) Tamanhos de chave a serem suportados: São suportadas chaves de 1024 bits, 2048 bits e 4096 bits.

7.2.2. Requisitos para um servidor TSP

7.2.2.1. Perfil para o formato do pedido

a) Parâmetros a serem suportados

i. não necessita suportar nenhuma extensão;

ii. deve ser capaz de tratar os campos opcionais reqPolicy, nonce, certReq.

b) Algoritmos a serem suportados: SHA256, SHA384, SHA512.

7.2.2.2. Perfil do formato da resposta

a) Parâmetros a serem suportados

i. o campo genTime deve ser representado até a unidade especificada na PCT;

ii. deve haver uma precisão mínima, conforme definido na PCT;

iii. o campo ordering deve ser configurado como falso ou não deve ser incluído na resposta;

iv. extensão, não crítica, contendo informação sobre o encadeamento de carimbos do tempo, caso a ACT adote esse mecanismo;

v. outras extensões, se incluídas, não devem ser marcadas como críticas;

vi. campo de identificação do alvará vigente no momento da emissão do CT.

b) Algoritmos a serem suportados: SHA256, SHA384, SHA512.

c) Tamanhos de chave a serem suportados: São suportadas chaves de 2048 bits e 4096 bits

7.2.3. Perfil do Certificado do SCT

7.2.3.1. A ACT Certisign assina cada mensagem de carimbo do tempo com uma chave privada específica para esse uso. A ACT Certisign usa chaves distintas para acomodar, por exemplo, diferentes políticas, diferentes algoritmos, diferentes tamanhos de chaves privadas ou para aumentar a performance.

7.2.3.2. O certificado correspondente contem apenas uma instância do campo de extensão, conforme definido na RFC 5280, com o sub-campo KeyPurposeID contendo o valor id-kp-timeStamping. Essa extensão é crítica.

7.2.3.3. O seguinte OID identifica o KeyPurposeID, contendo o valor id-kp-timeStamping: 1.3.6.1.5.5.7.3.8.

7.2.4. Formatos de nome

O certificado digital emitido para o SCT da ACT Certisign adota o "Distinguished Name" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

O = ICP-Brasil

OU = Autoridade de Carimbo de Tempo Certisign

CN = < nome do Servidor de Carimbo do tempo >

7.3. Protocolos de transporte

O serviço será disponibilizado por meio do protocolo TSP (conforme descrito na RFC 3161), onde o cliente deve enviar uma solicitação de carimbo (timestamp query). O protocolo TSP é disponibilizado utilizando como meio de transporte o protocolo HTTPS com autenticação cliente.

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

Os itens seguintes definem como será mantida e administrada a DPCT.

8.1. Procedimentos de mudança de especificação

Alterações nesta DPCT são solicitadas e/ou definidas pelo Grupo de Práticas e Políticas da ACT Certisign. Novas versões serão igualmente submetidas à aprovação da AC Raiz.

Esta DPCT é atualizada sempre que uma nova PCT implementada pela ACT Certisign o exigir.

8.2. Políticas de publicação e notificação

A ACT Certisign mantém página específica com a versão corrente desta DPCT para consulta pública, a qual está disponibilizada no endereço Web: http://icp-brasil.certisign.com.br/repositorio/act-certisign/index.htm.

8.3. Procedimentos de aprovação

Esta DPCT da ACT Certisign foi submetida à aprovação, durante o processo de credenciamento da ACT Certisign, conforme determinado em CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [5].

Novas versões serão igualmente submetidas à aprovação da AC Raiz.

9. DOCUMENTOS REFERENCIADOS

9.1 Os documentos abaixo são aprovados por Resoluções do Comitê Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[1]	VISÃO GERAL DO SISTEMA DE CARIMBO DO TEMPO NA ICP-BRASIL	DOC-ICP-11
[2]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CARIMBO DO TEMPO NA ICP-BRASIL	DOC-ICP-13
[3]	PROCEDIMENTOS PARA AUDITORIA DO TEMPO NA ICP-BRASIL	DOC-ICP-14
[4]	POLITICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02
[5]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[6]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[7]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[8]	POLÍTICA TARIFÁRIA DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL	DOC-ICP-06
[9]	REGULAMENTO PARA HOMOLOGAÇÃO DE SISTEMAS E EQUIPAMENTOS DE CERTIFICAÇÃO DIGITAL NO AMBITO DA ICP-BRASIL	DOC-ICP-10
[10]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01
[11]	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL	DOC-ICP-12

10. REFERÊNCIAS

BRASIL, Decreto nº 4.264, de 10 de junho de 2002 - Restabelece e Modifica o Regulamento anterior.

BRASIL, Lei nº 9.933, de 20 de dezembro de 1999 - Dispõe sobre o Conselho Nacional de Metrologia, Normalização e Qualidade Industrial (CONMETRO) e sobre o Instituto Nacional de Metrologia, Normalização e Qualidade Industrial (INMETRO).

RFC 1305, IETF - Network Time Protocol version 3.0.

RFC 2030, IETF - Simple Network Time Protocol (SNTP) version 4.0.

RFC 2527, IETF - Internet X-509 Public Key Infrastructure Certificate Policy and Certifications Practices Frame work, março de 1999.

RFC 3161, IETF - Public Key Infrastructure Time Stamp Protocol (TSP), agosto de 2001.

RFC 3628, IETF - Policy Requirements for Time Stamping Authorities, November 2003.

ETSI TS 101.861 - v 1.2.1 Technical Specification / Time Stamping Profile, março de 2002.

ETSI TS 102.023 - v 1.1.1 Technical Specification / Policy Requirements for Time Stamping Authorities, abril de 2002.