

Universidade Católica de Brasília
Pró-Reitoria de Pós-Graduação e Pesquisa

MBA em Gestão de Sistemas de Informação

Segurança da Informação

Cartório Eletrônico

Prof: Ly Freitas

Equipe: Eliza Aiko Otake

Marcelo Lins Faustino

Nildo Nunes Cornélio

Novembro de 2002

Cartório Eletrônico

Eliza Aiko Otake

Marcelo Lins Faustino

Nildo Nunes Cornélio

Resumo

Com o crescimento do número e da variedade das transações de toda ordem na internet, é cada vez mais forte a necessidade de se garantir a segurança na troca de dados entre os navegadores e os servidores web. O protocolo mais utilizado para tal finalidade é o HTTP que não oferece as características de segurança necessárias para uma transação comercial. Para contornar esse problema, usa-se o protocolo SSL (Secure Sockets Layer) que tem como característica principal o estabelecimento de um canal privado (os dados são cifrados), autenticado (o servidor e o cliente podem ser autenticado) e confiável (o transporte de uma mensagem inclui uma verificação de integridade). A autenticação feita pelo SSL é realizada com a utilização de um Certificado Digital, que pode ser considerado como uma identidade digital. Estes Certificados Digitais são emitidos por entidades confiáveis conhecidas como Autoridades Certificadoras. Este trabalho envolve a conceituação de certificação eletrônica e as práticas adotadas pela Autoridade Certificadora do Serpro (Serviço Federal de Processamento de Dados).

Palavras-chave

Assinatura digital, Chaves Públicas, Certificação Digital, Autoridade Certificadora.

Electronic Registry

Summary

With the rising of the number and varieties of every kind of transactions in the internet, the need of assure the security in data exchange among the navigators and web servers is stronger and stronger. The most used protocol to get to this goal is HTTP, wich doesn't offer the security features needed to a commercial transaction. To solve this problem, man use the SSL (Secure Sockets Layer) protocol, wich have as a main feature the stabilishment of a private channel (the data are written in code), authenticated (the server and the cliente can be authenticated) and trustable (the transport of a message includes a integrity verification). The authentication is done by SSL with one Digital Certificate, wich can be considered as a digital identity. These Digital Certificates are emitted by trustable entities known as Certifiers Authorities. This work deals with the conception of electronic certification and the practices adopted by the Certifier Authority of Serpro (Brazilian Federal Service).

Keywords

Digital signature, Public keys, Digital Certificate, Certifier Authority.

1. Histórico

Os Estados Unidos foram os pioneiros no uso da tecnologia da assinatura digital. Em 1995, o Estado de Utah foi o primeiro a legalizar esse tipo de tecnologia. Em junho de 2000, o presidente Clinton, usando um software para assinatura digital (o Lexign ProSigner) assinou o Electronic Signatures in Global and National Commerce Act, que legalizou essa prática naquele País, tal como no Brasil. Embora com um pouco de atraso, a União Européia, através do seu Parlamento, tomou caminho similar: foi emitido o Comunicado European Framework for Digital Signatures and Encryption, que obrigou todos Países membros a se adequarem a esse tipo de tecnologia até janeiro de 2002.

O Brasil também já dispõe da sua Infra-estrutura de Chave Pública (ICP), criada pela Medida Provisória nº 2.200, de 28 de junho de 2000.

A implantação da ICP-Brasil faz parte de um conjunto de serviços necessários para o uso de tecnologia de criptografia de chave pública e de assinatura digital em larga escala. Embora o conceito de criptografia por chaves públicas seja antigo, apenas recentemente surgiram soluções comerciais que permitem a sua implementação de forma efetiva. O propósito principal da ICP é a gestão das chaves e dos certificados para uso em criptografia e assinatura digital.

É interessante deixar claro que o novo sistema de certificação eletrônica não introduz conceitos novos nas transações, apenas estabelece equivalência e isonomia legal entre os documentos produzidos e obtidos eletronicamente e os documentos firmados em papel, desde que certificados na ICP-Brasil. Isso significa que as certificações realizadas por entidades certificadoras não vinculadas a ICP-Brasil poderão continuar sendo feitas.

Nessa condição, ao certificar determinado documento, as entidades o atestam quanto a sua autenticidade e integridade, de modo semelhante a uma testemunha. Já no caso de uma entidade certificadora vinculada ao sistema ICP-Brasil, seus documentos gozarão de uma presunção de autenticidade derivada da lei.

A partir de então, as empresas certificadoras passam a ter a opção de estarem ligadas ou não ao ICP-Brasil, dependendo das suas necessidades. Caso a opção seja participar do ICP, a única condição é que sejam cumpridas as regras estabelecidas na Medida Provisória e pelo Comitê Gestor. A decisão tem vantagens e desvantagens: ao mesmo tempo que dá mais credibilidade a unidade certificadora e pressupõe validade, também significa mais custos.

Os especialistas não cansam de alertar as empresas, públicas ou privadas, de que a certificação digital é uma ferramenta com enorme potencial para aumentar a segurança, mas que requer altos investimentos. É uma solução aparentemente simples, mas exige das empresas preparo para criar uma estrutura capaz de sustentar o novo tipo de aplicação. Nesse sentido, o passo dado pelo governo é encarado com

otimismo pelo setor privado só prova que o poder público está atento a questão de segurança, apesar dos problemas burocráticos que a envolvem.

Apenas para se ilustrar o que foi dito anteriormente, o Serpro, escolhido para ser a autoridade certificadora raiz do ICP-Brasil investiu R\$ 7 milhões para atender os requisitos solicitados pelo ITI (Instituto Nacional de Tecnologia da Informação), e a AC-raiz está instalada em uma sala-cofre especialmente construída dentro da regional do Rio de Janeiro. O Serpro aproveitou as suas instalações e, se assim não fosse, a demanda de investimentos subiria para algo em torno de R\$ 25 milhões.

Abaixo encontra-se representada a evolução histórica da certificação digital no Brasil:

13/06/2000: Decreto 3.505, com a instituição da Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

05/09/2000: Decreto 3.587, que estabeleceu normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal – ICP-gov. Nele ficou definido que a criptografia utilizaria duas chaves matematicamente relacionadas, onde uma delas é pública e, a outra, privada, para criação de assinatura digital.

17/11/2000: Como uma corporação de Tecnologia da Informação, o Serpro se adequou aos padrões internacionais de segurança (ISO 17799) e demais padrões de mercado praticados no mundo para instalações desse porte e se tornou Autoridade Certificadora. O Serpro foi escolhido para operar a AC-Raiz porque dispõe e opera de infra-estrutura adequada, constituída de pessoal qualificado, instalações, equipamentos e softwares específicos, com nível de segurança internacionais.

28/06/2001: Medida Provisória 2.200, legaliza a assinatura eletrônica no País.

27/07/2001: Medida Provisória 2.200-1 instituiu o ICP-Brasil que possibilita a habilitação de instituições públicas e organismos privados para atuarem na validação jurídica de documentos produzidos, transmitidos ou obtidos sob a forma eletrônica. Com essa medida passa-se a dispor de alternativa para realizar eletronicamente transações que até agora não se podiam fazer e exigiam registros em papel escrito para adquirirem validade. Na realidade o novo sistema de certificação eletrônica não introduz conceitos novos nas transações, apenas estabelece equivalência e isonomia legal entre os documentos produzidos e obtidos eletronicamente e os documentos firmados em papel, desde que certificados na ICP-Brasil.

24/08/2001: Assinatura entre o Serpro e o Instituto Nacional de Tecnologia da Informação – ITI – do Ministério da Ciência e Tecnologia de contrato para prestação de serviços de Autoridade Certificadora Raiz (AC-Raiz) que compõe a Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil).

2. Conceitos Básicos

2.1. Assinatura Digital

É a tecnologia que permite conduzir transações eletrônicas seguras por meio da Internet, ou em ambientes correlatos, como intranets/extranets. Essas transações passaram a ser de grande importância para grande número de organizações, tanto públicas, como privadas, por sua conveniência, baixo custo e facilidade para tornar esse acesso universal. Uma das questões primordiais, entretanto, é garantir a segurança e a integridade dessas transações, em particular a possibilidade de assinar as transações. A tecnologia que dá essa garantia é chamada de assinatura eletrônica (e-Sign), que pode ser feita diretamente em formulários eletrônicos ou em documentos diversos que caracterizem essas transações (contratos, cartas, memorandos, planilhas, etc.). A assinatura eletrônica não é, como poderia parecer a primeira vista, a digitalização da assinatura feita de próprio punho e sua “colagem” em documentos eletrônicos. É, na verdade, um sistema de códigos para identificação e autenticação do signatário, que é tratado por um software especialmente desenvolvido para essa finalidade.

2.2. Chaves Públicas

As chaves públicas são um par de chaves matematicamente relacionadas entre si de maneira bi-unívoca (A corresponde somente a B, e vice-versa), criptografadas, geradas ao mesmo tempo, sendo uma delas denominada de pública e outra de privada (secreta). A criptografia das chaves públicas permite que haja comunicação entre duas entidades, sem que se saiba a chave secreta.

A chave pública é sempre associada de forma segura a uma pessoa, programa, equipamento ou entidade. Assim, cada certificado contém, dentre outras informações, a identificação única do usuário descrito, o qual é o único que possui a chave secreta correspondente àquela chave pública. O certificado só será assinado eletronicamente depois que esse processo de identificação for concluído.

2.3. Infra-estrutura de Chaves Públicas

Uma infra-estrutura de Chaves Públicas (ICP) é um ambiente criado por um conjunto de tecnologias que permite garantir a segurança da assinatura de transações ou documentos eletrônicos, através do uso de um par de chaves, sendo uma delas pública (de conhecimento geral) e a outra privada (somente do conhecimento do seu proprietário), consolidadas num “certificado” digital. Esse certificado digital permite identificar, sem qualquer sombra de dúvida, as pessoas (física ou jurídica) que estejam conduzindo transações em ambiente eletrônico, de forma similar a um cartório, reconhecendo as assinaturas de um documento em papel.

2.4. Certificação Digital

É uma espécie de assinatura que permite a identificação de quem mandou a mensagem, sendo que essa assinatura dá-se em forma de documento eletrônico que possibilita a troca de informações entre duas partes dentro de padrões de segurança que permitam a autenticação da identificação por elas apresentadas. Cada certificado contém, dentre outras informações, a identificação única do usuário descrito, o qual é o único que possui a chave privada correspondente àquela chave pública.

Na prática, isso significa que o sistema permite aos usuários verificarem se são realmente aqueles que dizem ser, e uma das formas de obter essa confirmação é utilizar uma entidade confiável para autenticar a chave pública.

Os certificados digitais são conservados, pelas Autoridades Certificadoras, em repositórios que permitem acesso ao público, mediante consulta on line – esta é a forma de se verificar a validade de determinado certificado, usado para assinar certo documento. Uma possibilidade é conservar o certificado e a chave privada diretamente no microcomputador a partir de onde a transação é feita. Outra possibilidade é gravá-los num cartão magnético, que é lido pelo microcomputador que estiver conduzindo a transação. O cartão ou micro podem ter proteção adicional de senha ou de identificação digital, caso isto seja desejável. Por exemplo, os certificados digitais usados pelas mais altas autoridades do governo federal estão contidos em cartões, protegidos por senhas.

2.5. Autoridade Certificadora

A autoridade certificadora (CA – certificate authority) é uma empresa, pública ou privada, brasileira ou não, que representa uma entidade responsável pela emissão, gerenciamento, renovação e revogação dos certificados digitais.

A CA tem um papel básico de garantir a correspondência entre a identidade e a chave pública de uma determinada entidade, sabendo que tal chave pública corresponde a uma chave privada que permanece sob guarda exclusiva dessa entidade.

Para tanto, a CA deve ser capaz de realizar todos os processos de emissão de certificados, verificação de validade, armazenamento, publicação ou acesso on-line, revogação e arquivamento para verificação futura. Em consequência, uma autoridade certificadora constitui-se de um sistema computacional completo, com capacidade de comunicação, processamento e armazenamento. Além disso, tanto as comunicações envolvendo esse sistema, assim como o próprio sistema, devem ser também protegidos e a própria identidade do sistema deve ser garantida, necessidade esta que são atendidas por intermédio da publicação de uma chave pública pertencente a própria autoridade certificadora. Como tal chave deve também ser garantida com um certificado digital, então, em geral, uma autoridade certificadora

deposita sua chave pública junto a outra autoridade certificadora, formando uma

estrutura de certificação onde algumas CA funcionam como autoridades certificadoras para outras CAs.

Como mostrado anteriormente, um problema fundamental, o qual coloca em risco ambientes abertos com grande número de participantes que não se conhecem, é a questão da autenticidade da chave pública. Sem garantias adicionais, cada entidade usuária deverá desenvolver a sua verificação de autenticidade para cada chave pública das outras entidades com quem deseja comunicar-se antes de confiar nessas outras entidades. A complexidade desse problema pode ser reduzida pela certificação da chave pública de uma determinada entidade por intermédio de uma terceira parte em que ambos, emissor e receptor, confiem. Essa terceira parte, chamada de Autoridade Certificadora – CA, assina um certificado contendo a chave pública de uma entidade usuária, mais alguns dados adicionais tais como o nome da entidade, o período de validade do certificado, etc. A assinatura da CA é realizada com um algoritmo de assinatura digital usando a chave secreta da própria CA, de modo que tal assinatura pode ser verificada por qualquer entidade usando a chave pública da CA. O certificado assinado pela CA é chamado Certificado Digital.

A necessidade de que uma CA tenha sua chave reconhecida ou assinada por uma outra CA leva a estruturação de uma hierarquia de CA para certificação de chaves públicas de criptografia. A CA que se encontra no topo de uma hierarquia tem uma característica especial: ela recorre a si mesma para certificar sua chave pública.

Vale observar que um certificado é gerado a partir de uma solicitação feita por alguma entidade a uma CA. A solicitação, após uma validação da identidade do solicitante através de algum processo com presença física ou com alguma troca de informação via rede, é atendida com a emissão do certificado contendo a assinatura da CA, assinatura esta que validará a identidade da entidade indicada no certificado.

No caso da emissão do certificado da CA de nível mais alto de uma hierarquia de CA (CA root/ CA-raiz), a própria autoridade assinará o seu certificado. Neste único caso, o certificado é auto-assinado e, assim, o emissor do certificado é o mesmo que o receptor.

Algumas autoridades certificadoras e hierarquias de certificação encontram-se em operação para serviços de comunicação na Internet e especificamente para aplicações web que envolvem compras e pagamentos ou trocas de informações reservadas. Por essa razão, vários navegadores web são pré-configurados para confiar em autoridades certificadoras bem conhecidas, isto é, tais navegadores já vem com os certificados de autoridades como a VeriSign, Thawte, dentre outras.

Por isso, ao se criar uma autoridade certificadora própria, faz-se necessário estabelecer um processo para enviar aos browsers o certificado dessa autoridade, habilitando os browsers para validar certificados assinados por tal autoridade certificadora.

3. Requisitos para instalação da assinatura eletrônica

Autenticidade, isto é, o estabelecimento, de forma inequívoca, da identidade das pessoas (físicas ou jurídicas) que estão assinando a transação ou os documentos a ela anexos.

Não-repudição, isto é, a garantia de que nenhuma das partes pode repudiar uma transação ou os documentos correspondentes, que tenham sido legitimamente assinados.

Referência da data em que a assinatura de cada parte se deu.

Integridade, isto é, garantia de que o conteúdo dos documentos que estão sendo visualizados é exatamente o mesmo que foi assinado pelas partes.

Auditoria, isto é, a capacidade de reconstruir, a qualquer momento, toda a cadeia de eventos relacionados com a assinatura dos documentos ou da transação, exatamente da forma como ela ocorreu.

4. Diferença entre assinatura eletrônica e infra-estrutura de Chaves Públicas.

Enquanto a ICP trata da emissão dos certificados digitais e, conseqüentemente, do par de chaves a eles associados, a tecnologia de assinaturas eletrônicas lida com essas chaves para proporcionar várias funções como a realização da assinatura propriamente dita (autorização/aprovação), a verificação da identidade dos signatários e dos seus poderes para tanto (por exemplo, no caso de procurações) e da integridade do conteúdo que estiver sendo visualizado (em relação ao que foi assinado).

5. Garantia da segurança da assinatura eletrônica com a ICP.

No ato da assinatura, o software para assinatura eletrônica gera um código matemático, a partir de um algoritmo para “embrulho” do conteúdo do documento ou formulário que estiver sendo assinado. O código gerado, conhecido como “resumo”(hashing), é único para cada processo e conteúdo – como se fosse a impressão eletrônica digital daquele documento ou formulário. A chave privada do remetente é, então, utilizada para codificar (criptografar) esse código. A esse processo todo, tecnicamente, dá-se o nome de assinatura eletrônica. Como foi utilizada a chave privada do remetente durante o processo de assinatura, ela está diretamente vinculada ao remetente.

O documento assinado é, então, enviado por meio eletrônico (por exemplo, através de e-mail), a quem de direito, juntamente com a chave pública do remetente. Quando o destinatário recebe o documento, precisa verificar a autenticidade da assinatura e a integridade do conteúdo, ou seja, assegurar-se que nenhuma modificação tenha sido nele introduzida após a assinatura. A chave pública do remetente é usada para decodificar (reverter a criptografia). Para tanto, o mesmo algoritmo de “embrulho” é aplicado ao conteúdo para gerar um novo “resumo”. Esses dois “resumos” (o original e o novo) são então comparados: se forem idênticos, a validação do conteúdo é feita. Se tiverem sido feitas alterações no conteúdo do documento, após sua assinatura, o “resumo” gerado na verificação irá diferir do original e uma mensagem de não validação será apresentada ao usuário.

Caso o remetente criptografe o texto de mensagem com a chave pública do destinatário, somente este conseguirá decifrá-la, usando a sua chave secreta, e ambos terão certeza da confidencialidade da mensagem. Quando o destinatário envia um recibo de uma mensagem para o remetente, criptografado com a chave pública deste, somente ele poderá decifrá-lo e assim ambos não poderão negar o envio e a recepção de mensagem, ao que damos o nome de irretratabilidade ou não perjúrio.

O software de assinatura também faz a verificação da validade do certificado digital utilizado, por meio de uma consulta (feita automaticamente) ao site da Autoridade Certificadora correspondente, onde são verificados a data de validade, os poderes de assinatura etc. As três verificações (identidade do remetente, validade do certificado e integridade do conteúdo), acopladas a informação da data em que a assinatura foi feita, complementam o pacote de controles que precisam ser obrigatoriamente feitos para garantir a segurança da transação.

6. Autoridade Certificadora do Serpro

Serão abordadas a seguir determinadas práticas de certificação da Autoridade Certificadora do Serpro, a qual utiliza o ambiente e os serviços do Centro de Certificação Digital do Serpro (CCD Serpro) para hospedar, operar e dar manutenção à ACSERPRO.

A ACSERPRO mantém página WEB <https://thor.serpro.gov.br/ACSERPRO>, que contém as seguintes informações: DPC (Declaração de Práticas de Certificação); PC (políticas de certificação) que implementa; Certificado da ACSERPRO e Certificado da AC Raiz da ICP-Brasil, cuja disponibilidade é de, no mínimo, de 99% (noventa e nove por cento), 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

São publicadas sempre as versões mais recentes aprovadas da DPC e PC pertinentes prontamente após a aprovação.

A publicação das LCR é disponibilizada conforme definido em cada PC que a ACSERPRO implementa.

Os Certificados são publicados prontamente conforme sua geração e emissão nos casos em que as PC assim o definirem.

Não há nenhum controle de acesso na leitura da DPC ou de PC pertinente nas páginas web nomeadas para publicação.

São utilizados controles de acesso apropriados para restringir a possibilidade de escrita ou modificação destes documentos a pessoal autorizado.

A ACSERPRO adota como repositório de LCR uma página WEB <http://thor.serpro.gov.br/LCR/ACSERPRO.crl> <http://thor.serpro.gov.br/LCR/LCRSERPRO-SPB.crl>, que atende aos seguintes requisitos: Disponibilidade, Protocolos de acesso – HTTP e HTTPS e Requisitos de Segurança.

6.1. Sigilo

A chave privada de assinatura digital da ACSERPRO é gerada e mantida pela própria ACSERPRO, que é responsável pelo seu sigilo.

Os titulares de certificados de assinatura digital emitidos pela ACSERPRO são responsáveis pela geração, manutenção e pela garantia do sigilo de suas respectivas chaves privadas, bem como pela divulgação ou utilização indevidas dessas mesmas chaves.

Todas as informações coletadas, geradas, transmitidas e mantidas pela ACSERPRO são consideradas sigilosas, exceto os certificados de chaves públicas e LCR, os quais são considerados não sigilosas, assim como a versão da DPC da ACSERPRO ou das PC por ela implementadas.

Essas informações são arquivadas de acordo com sua classificação que estão especificadas no Manual de Segurança.

Como princípio geral, nenhum documento, informação ou registro fornecido a ACSERPRO ou as AR deverá ser divulgado.

É considerado que todos os registros de solicitação são informações sigilosas, incluindo:

- solicitações de Certificados, aprovadas ou rejeitadas;
- documentos ou detalhes da prova de identificação do solicitante;
- informações coletadas como parte dos registros de solicitação. Isto não impede a publicação de informação de certificado exigida em diretório ou página web da ACSERPRO;

- contrato de assinante.

- qualquer informação solicitada de um terceiro para operar uma AR dentro da cadeia de confiança da ACSERPRO.

A razão pela qual um certificado é revogado é considerada sigilosa, com a exceção exclusiva da revogação de certificados de AR devido a:

- comprometimento da Chave Privada, em casos onde se possa revelar que a Chave Privada foi comprometida;
- terminação da AR, no caso em que a divulgação prévia da terminação seja permitida.

6.2. Informações não Sigilosas

Como princípio geral, nenhum documento, informação ou registro que pertençam ou estejam sob a guarda da ACSERPRO ou suas AR é divulgado a entidades legais ou seus funcionários, exceto onde existe uma ordem judicial corretamente constituída e está corretamente identificado o representante da lei.

Nenhum documento, informação ou registro sob a guarda da ACSERPRO e suas AR será fornecido a qualquer pessoa, exceto quando a pessoa que o requerer, por meio de instrumento devidamente constituído, estiver autorizada para fazê-lo e for corretamente identificada.

O Titular do Certificado, ou seu representante legal, poderá ter acesso a quaisquer dos seus dados ou identificações, ou poderá autorizar a divulgação de seus registros a outras pessoas. Para tanto, a solicitação de liberação de informação deverá ser acompanhada de autorização formal do Titular do Certificado.

Nenhuma outra liberação de informação, que não as expressamente descritas acima, é permitida.

6.3. Tarifas

Os seguintes serviços são tarifados: emissão ou renovação de certificados e revogação ou acesso a informação de estado.

Os seguintes serviços não possuem incidência de tarifas: acesso ao certificado e outros serviços como informação de política.

Não há política de reembolso.

6.4. Obrigações e Direitos

Dentro das fontes de pesquisas realizadas, foram levantadas as obrigações da Autoridade Certificadora do SERPRO - ACSERPRO, as Autoridades de Registro - AR vinculadas e a dos titulares de certificados, cabendo destacar aquelas de maior relevância na visão do grupo de trabalho:

ACSERPRO:

- operar de acordo: - com a Declaração de Práticas de Certificação da Autoridade Certificadora do SERPRO, a qual é publicada em sua página web, com as Políticas de Certificado que implementa, com a Política de segurança da Infra-estrutura de Chaves Públicas do Brasil (ICP-Brasil), com a Política de segurança e procedimentos operacionais da ACSERPRO.
- gerar e gerenciar o seu par de chaves criptográficas.
- assegurar proteção de sua chave privada.
- notificar a AC Raiz da ICP-Brasil quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação desse certificado.
- notificar os seus usuários quando ocorrer suspeita de comprometimento de sua chave, emissão de novo par de chaves e correspondente certificado, ou o encerramento de suas atividades.
- emitir, expedir e distribuir os certificados de AR vinculadas e de titulares de certificados.
- emitir, gerenciar e publicar na página web suas listas de certificados revogados (LCR).
- investigar comprometimento e suspeitas de comprometimento de sua chave privada.

Autoridades de Registro:

- operar de acordo: - com a Declaração de Práticas de Certificação da Autoridade Certificadora do SERPRO, com as Políticas de Certificado a qual se vincula, com a Política de segurança da Infra-estrutura de Chaves Públicas do Brasil (ICP-Brasil), com a Política de segurança e procedimentos operacionais da ACSERPRO.
- receber solicitações de emissão ou de revogação de certificados.
- confirmar a identidade do solicitante e a validade da solicitação.
- disponibilizar os certificados emitidos pela ACSERPRO aos seus respectivos solicitantes.

Titulares de Certificados:

- fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação.
- garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos de acordo com as recomendações previstas na PC correspondente.
- informar à ACSERPRO, através de sua AR, qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

- assinar o termo de responsabilidade do certificado.

Com relação aos DIREITOS, estes foram identificados para os Usuários de Certificados, ou seja, entidades que confiam no teor, validade e aplicabilidade do certificado digital, sendo eles: verificar, a qualquer tempo, a validade do certificado e recusar a utilização do certificado para fins diversos dos previstos na Política de Certificado correspondente. No tocante a eventuais indenizações pelos usuários de certificados não existe esta prática, exceto na prática de ato ilícito.

6.5. Responsabilidades

As responsabilidades da ACSERPRO, consistem:

- adotar as medidas de segurança e controle previstas na Declaração de Práticas de Certificação da Autoridade Certificadora do SERPRO, nas Políticas de Certificados e de Segurança, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil.
- manter e garantir a integridade, sigilo e a segurança da informação por ela tratada.
- manter e testar regularmente seu Plano de Continuidade do Negócio.
- informar às terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil que será contratada pela ACSERPRO quando uma de suas PC assim o exigir.

No caso das Autoridades de Registro (AR) vinculadas, cabe manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras estabelecidas pela ACSERPRO, bem como manter e garantir a segurança da informação por ela tratada, de acordo com as normas, critérios, práticas e procedimentos da ICP-Brasil.

6.6. Controle de Segurança Física

A localização e o sistema de certificação utilizado para a operação da ACSERPRO não são publicamente identificados, fato que dificultou nosso trabalho de pesquisa.

Foi identificado que o acesso às instalações dos equipamentos utilizados para a operação da Autoridade Certificadora do SERPRO - ACSERPRO só é permitido a pessoas autorizadas, cujo controle dá-se através de cartões magnéticos, senhas e identificação biométrica. Os tipos de acesso físico são divididos em 04 (quatro) níveis e mais 02 (dois) níveis relativos à proteção da chave privada de AC.

No nível 1, nenhum tipo de processo operacional ou administrativo da ACSERPRO é executado, cujo controle de acesso ocorre por identificação e registro

por funcionário da segurança. A partir desse nível, equipamentos de gravação, fotografia, celulares, vídeo, som e notebook não são permitidos, salvo com autorização formal e supervisão. O acesso ao segundo nível exige identificação de duas pessoas autorizadas por meio eletrônico e o uso de crachá. No terceiro nível encontram-se as atividades relativas ao ciclo de vida dos certificados digitais, motivo pelo qual pessoas não envolvidas neste tipo de atividade não têm permissão de acesso, salvo em caso de estarem acompanhadas por funcionário designado. Neste nível são controladas por cartão eletrônico e identificação biométrica tanto as entradas e saídas de cada pessoa.

No nível 4 situa-se a chamada “sala cofre”, onde as paredes, piso e teto são revestidos de aço e concreto a prova de água, vapor, gases e fogo. Os dutos de refrigeração, energia e de comunicação não permitem a invasão física desta área. Na “sala cofre” ocorrem as atividades sensíveis da ACSERPRO, como por exemplo a emissão e revogação de certificados. Os critérios para o acesso físico são os mesmos do nível 3, exigindo-se adicionalmente a identificação de no mínimo duas pessoas autorizadas.

Os níveis 5 e 6 são internos dos ambientes de nível 4, compreendendo aos cofres ou gabinetes propriamente ditos e pequenos depósitos localizados no interior destes, os quais possuem fechaduras individuais. As chaves privadas são armazenadas nesses depósitos.

Todo esse ambiente é monitorado 24 horas/7 dias por semana ininterruptamente por câmeras de vídeo, cujos posicionamentos estratégicos não permitem visualizar a digitação de senhas nos controles de acesso. As portas de acesso entre os níveis 3 e 4 são monitoradas, também, por sistema de alarmes sonoro e visual. O ambiente de quarto nível possui, inclusive, um alarme de detecção de movimento, o qual é reativado automaticamente na saída de um ou mais funcionários de confiança daquele ambiente.

Na falta de energia o ambiente funcionará temporariamente utilizando nobreaks com autonomia suficiente até o acionamento do gerador de apoio. O sistema de ar condicionado, o qual controla o calor e umidade, é independente do sistema do edifício, cujo controle é monitorado por alarmes.

Documentos em papel ou em mídia magnética que contêm elementos confidenciais, são eliminados por triturador de papéis ou por um método aprovado para esfregar ou sobrescrever a mídia magnética.

6.7. Controle de Segurança Procedimental

Uma das práticas utilizadas é a separação das tarefas para funções críticas, a fim de evitar que o funcionário utilize indevidamente o sistema sem ser detectado.

Todos os operadores recebem treinamento antes de obter qualquer tipo de acesso, sendo que o tipo e o nível para o acesso são determinados, em documento formal, com base nas necessidades de cada perfil.

Os perfis/funções estabelecidos pela ACSERPRO são:

- Gerente do CCD.
- Administrador de segurança.
- Administrador de banco de dados.
- Administrador do sistema de gerenciamento de certificados.
- Administrador do servidor WEB.
- Administrador do sistema Unix.
- Administrador do security sever.
- Administrador de AC.
- Operador.
- Operador de autoridade de registro.
- Segurança patrimonial.
- Apoio administrativo.

Quando há mudança de função do empregado, as permissões de acesso são revistas. Em caso de desligamento do empregado, as permissões de acesso são revogadas imediatamente.

Indivíduos separados podem cobrir simultaneamente até três dos papéis/perfis acima descritos, separando-se por natureza da operação como por exemplo o administrador de segurança, o qual tem que permanecer separado do administrador de sistema para prover uma revisão independente dos logs de auditoria.

6.8. Controle de Pessoal

A fim de resguardar a segurança e a credibilidade da ACSERPRO, todas as pessoas que venham a ocupar os perfis estabelecidos, passam por um processo rigoroso de seleção, onde verificados antecedentes criminais, situação de crédito, histórico de empregos anteriores, comprovação de escolaridade e residência, qualificação e experiência.

Atendidos esses critérios de seleção, os funcionários terão registrado em contrato ou termo de responsabilidade o compromisso de observar as normas, políticas e regras aplicáveis da ACSERPRO e ICP-Brasil e de não divulgar informações sigilosas a que tenham acesso. Eventual descumprimento ou ações não autorizadas são

submetidas a autoridades internas que após avaliação, podem resultar desde a suspensão de acesso até a medidas outras administrativas e legais.

Todo o pessoal da ACSERPRO e das AR vinculadas, envolvido em atividades diretamente relacionadas com o processo de certificados (emissão, expedição, distribuição, revogação e gerenciamento), recebem treinamento documentado acerca de temas que envolvam os princípios e mecanismos de segurança, sistema de certificação, procedimentos de recuperação de desastres e de continuidade do negócio e outros assuntos correlacionados.

A ACSERPRO não implementa rodízios de cargos, pelo próprio princípio dos critérios procedimentais.

6.9. Segurança Lógica e Auditoria

Todas as AR (Autoridades Registradoras) vinculadas ao SERPRO são obrigadas por contrato AC (Autoridade Certificadora) – AR a manter registros e arquivos com informações sobre todas as operações realizadas e trilhas de auditoria geradas para fins de auditoria.

A ACSERPRO (Autoridade Certificadora do SERPRO) registra em arquivos para fins de auditoria todos os eventos relacionados à segurança do seu sistema de certificação:

- Iniciação e desligamento do sistema de certificação;
- Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da ACSERPRO;
- Mudanças na configuração da ACSERPRO ou nas suas chaves;
- Tentativas de acesso (*login*) e de saída do sistema (*logout*);
- Tentativas não autorizadas de acesso aos arquivos de sistema;
- Geração de chaves próprias da ACSERPRO ou de chaves de Titulares de Certificados;
- Emissão e revogação de certificados;
- Geração de LCR (Lista de Certificados Revogados);
- Tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas, e de atualizar e recuperar suas chaves;
- Operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável;
- Operações de escrita nesse repositório, quando aplicável;
- Mudanças na política de criação de certificados.

A ACSERPRO registra, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação:

- Registros de acessos físicos;
 - Manutenção e mudanças na configuração de seus sistemas;
 - Mudanças de pessoal e de perfis qualificados;
 - Relatórios de discrepância e comprometimento; e
-
- Registros de destruição de meios de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

Os registros de auditoria mínimos a serem mantidos pela ACSERPRO incluem todos:

- Registros de inscrição, inclusive registros relativos a solicitações rejeitadas;
- Pedidos de geração de certificado, mesmo que a geração não tenha êxito;
- Registros de solicitação de emissão de LCR.

Todos os registros de auditoria, eletrônico ou manual, contém a data e a hora do evento registrado e a identidade do agente que o causou. Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços da ACSERPRO deverá ser armazenada, eletrônica ou manualmente, em local único, conforme a Política de Segurança da ICPBrasil (Infra Estrutura de Chaves Públicas do Brasil).

6.10. Frequência de auditoria de registros (logs) e período de retenção

A periodicidade de auditoria de registros não será superior a uma semana, sendo que os registros de auditoria são analisados pelo pessoal operacional da ACSERPRO. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros verificando-se que não foram alterados, em seguida procede-se a uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

A ACSERPRO mantém localmente, nas instalações do SERPRO/RJ, os seus registros de auditoria por pelo menos 2 (dois) meses e, subseqüentemente, faz o armazenamento.

6.11. Proteção de registro (log) de Auditoria

Os equipamentos da ACSERPRO, onde são gerados os diversos registros de sistemas pelo sistema operacional, banco de dados e do aplicativo de AC, encontram-se fisicamente em um ambiente classificado como nível 4 de segurança.

A inspeção contínua dos diversos registros dos sistemas é feita por meio das ferramentas nativas do sistema operacional, banco de dados e do aplicativo de AC, e estão disponíveis somente para leitura. Pode ser feita também por relatórios emitidos a partir destas ferramentas. Estes dados de auditoria são coletados e armazenados periodicamente em uma sala de arquivos, de nível de segurança 3. O

responsável por essa inspeção é o Administrador de Segurança da ACSERPRO ou seus designados.

Os registros de auditoria gerados eletrônica ou manualmente são obrigatoriamente classificados e mantidos conforme sua classificação, segundo os requisitos da Política de Segurança da ICP-Brasil.

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

A ACSERPRO executa procedimentos de *backup* de todo o sistema de certificação (SISTEMA OPERACIONAL + APLICAÇÃO DE AC + BANCO DE DADOS) de duas formas:

Diariamente: cópia de segurança; e Semanalmente: cópia armazenada para processos de auditoria.

6.13. Sistema de coleta de dados de auditoria

O sistema de coleta de dados de auditoria da ACSERPRO é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação de ACSERPRO e AR, pelo sistema de controle de acesso e pelo pessoal operacional, conforme tabela abaixo:

Tipo de evento	Sistema de coleção	Registrado por
Sucesso e fracasso de tentativas a mudanças sistema operacional segurança parâmetros	Automático	Sistema operacional
Início e parada de aplicação	Automático	Sistema operacional
Sucesso e fracasso de tentativas de <i>log-in</i> e <i>log-out</i>	Automático	Sistema operacional
Sucesso e fracasso de tentativas para criar, modificar ou apagar usuários de sistemas autorizados	Automático	Sistema operacional
Sucesso e fracasso de tentativas para pedir, gerar, assinar, emitir ou revogar chaves e certificados.	Automático	AC ou software de AR
Sucesso e fracasso de tentativas para criar, modificar ou apagar informação de Titular de Certificado.	Automático	Software de AR
Logs de Backup e restauração	Automático e manual	Sistema operacional e pessoal de operações
Mudanças de configuração de sistema	Manual	Pessoal de operações
Atualizações de software e hardware	Manual	Pessoal de operações
Manutenção de sistema	Manual	Pessoal de operações
Mudanças de pessoal	Manual	Pessoal de operações
Registros de acessos físicos	Automático e manual	Software de controle de acesso e pessoal de operações

Tabela 1. – Tabela de Controle de Acesso

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

6.14. Avaliações de vulnerabilidade

Uma Avaliação de Riscos de Segurança foi realizada para a ACSERPRO. Esta avaliação cobre a incidência de riscos e ameaças que podem impactar na operação dos serviços de certificação.

São realizadas avaliações individuais de ameaças e avaliações de risco a cada entidade subordinada implementada (AR). Eventos que indiquem possível vulnerabilidade, detectados na análise periódica dos registros de auditoria da ACSERPRO, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas e registradas para fins de auditoria.

6.15. Arquivamento de Registros

As seguintes informações são registradas e arquivadas pela ACSERPRO e AR:

- solicitações de certificados;
- solicitações de revogação de certificados;
- notificações de comprometimento de chaves privadas;
- emissões e revogações de certificados;
- emissões de LCR;
- trocas de chaves criptográficas da ACSERPRO;
- informações de auditoria previstas no item 1.1
- correspondências formais.

Os períodos de retenção para cada registro arquivado são os seguintes: as LCR referentes a certificados de assinatura digital são retidas por, no mínimo, período igual ao do arquivamento dos respectivos certificados. As demais informações são retidas por, no mínimo, 6 (seis) anos. Períodos de retenção específicos são definidos nas PC implementadas pela ACSERPRO, quando necessário.

Mídias de arquivos são guardadas em local seguro, sendo que a proteção criptográfica das mídias, as vezes é adotada. Também são protegidas de fatores ambientais como temperatura, umidade, e magnetismo.

Todos os registros arquivados serão classificados e armazenados com requisitos de segurança compatíveis com essa classificação, conforme a Política de Segurança da ICP-Brasil.

6.16. Procedimentos para cópia de segurança (backup) de arquivos

Uma segunda cópia de todo o material arquivado é armazenada em ambiente protegido com nível 3 de segurança.

As cópias de segurança devem seguir os períodos de retenção definidos para os registros dos quais são cópias. É feita a verificação da integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

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

Os servidores da ACSERPRO estão sincronizados com a hora GMT fornecida pelo Observatório Nacional. Todas as informações geradas que possuam alguma identificação de horário recebem o horário em GMT, inclusive os certificados emitidos por esses equipamentos. No caso dos registros feitos manualmente, estes contêm a Hora Oficial do Brasil.

6.18. Sistema de coleta de dados de arquivo

O sistema de coleta de dados de arquivos da ACSERPRO é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação de AC e AR e pelo pessoal operacional. Ver tabela abaixo.

Tipo de evento	Sistema de coleção	Registrado por
Solicitações de certificados	Automático e manual	Software de AC/AR e pessoal de operações
Solicitações de revogação de certificados	Automático e manual	Software de AC/AR e pessoal de operações
Notificações de comprometimento de chaves privadas	Manual	Pessoal de operações
Emissões e revogações de certificados;	Automático	Software de AC/AR
Emissões de LCR	Automático	Software de AC/AR
Correspondências formais	Manual	Pessoal de operações

Tabela 2. – Tabela de Controle de Coleta de Dados

6.19. Procedimentos para obter e verificar informação de arquivo

A integridade dos arquivos da ACSERPRO e das AR é verificada:

- Na ocasião em que o arquivo é preparado;
- Semestralmente no momento de uma auditoria de segurança programada;
- Em qualquer outro momento quando uma auditoria de segurança completa é requerida.

Somente podem ter acesso às informações de arquivo de uma AR:

- Pessoas devidamente autorizadas por meio de instrumento devidamente constituído e corretamente identificada.
- Titulares de Certificados, ou seus representantes legais, mediante solicitação formal.

6.20. Troca de chave

Os certificados emitidos pela ACSERPRO, e as respectivas chaves criptográficas geradas por seus Titulares, possuem prazos de validade que inicia a partir do momento da geração do certificado. Expirado este prazo, novo par de chaves deve ser gerado pelo Titular e nova solicitação de certificados efetuada à ACSERPRO. Os prazos dos certificados emitidos pela ACSERPRO estão detalhados nas PC aplicáveis.

As AR da ACSERPRO se encarregam de avisar aos Titulares de Certificados antes da expiração dos seus certificados para que o processo de solicitação de novo certificado não cause impacto aos mesmos.

6.21. Contingência

A ACSERPRO estabelece e mantém documentação detalhada composta por:

- Plano de Contingência, incluindo o comprometimento de chaves, *hardware*, *software*, falhas de comunicações, e desastres naturais como fogo e inundação;
- Padrões de configuração, incluindo sistema operacional, *software* de anti-vírus e programas aplicativos específicos;
- Procedimentos de *backup*, arquivamento e armazenamento externo de segurança;

Provê a documentação a pedido:

- do CG da ICP-Brasil, quando da auditoria de práticas de DPC;
- de pessoas que administram a segurança ou auditoria de conformidade;

Provê treinamento apropriado a todo pessoal pertinente em contingência e procedimentos de recuperação de desastre;

Testa pelo menos anualmente seu Plano de Contingência e Recuperação de Desastre com a atividade de teste mínima que é a restauração completa dos serviços operacionais como segue:

- a plataforma operacional atual é desligada e desconectada de links de comunicação;

- sistema operacional, os programas aplicativos e os dados operacionais são restabelecidos sobre uma plataforma de *hardware* nova, com mídias de *backup* em conformidade com o padrão de configuração;
 - serviço restabelecido é conectado aos links de comunicação e a operação correta de seus serviços de certificado é testada;
 - são retomadas as operações de serviço usando a plataforma operacional original. Tudo arquivado no disco rígido da plataforma de teste é apagado com segurança;
-
- Plano de Contingência e Recuperação de Desastre é revisado após os resultados do teste.

A ACSERPRO possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que recursos computacionais, *software* e/ou dados são corrompidos, e que podem ser resumidas no seguinte:

- É feita a identificação de todos os elementos corrompidos;
- O instante do comprometimento é determinado e é crítico para invalidar as transações executadas depois aquele instante.
- É feita uma análise do nível do comprometimento para a determinação das ações a serem executadas, que podem variar de uma simples restauração de um *backup* de segurança até a revogação do certificado da ACSERPRO.

A ACSERPRO possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que o certificado da entidade (ACSERPRO ou AR) tenha que ser revogado, e que podem ser resumidas no seguinte:

O Certificado da ACSERPRO é revogado:

- A AC Raiz é informada por comunicações seguras.
- A revogação é processada;
- A AC Raiz publica uma nova LCR imediatamente;
- São notificados os titulares e usuários de certificado;

A ACSERPRO pede um novo certificado à AC Raiz:

- A ACSERPRO revoga os certificados de AR antigos;
- Um novo par de chaves é gerado e a chave pública é entregue de maneira segura à AC Raiz para certificação;
- A AC Raiz valida o pedido de certificado e emite um novo certificado de AC;
- Procedimentos de *backup* de chaves privadas são executados;

Emitem-se novos certificados de AR:

- Cada AR submete um pedido para um certificado novo;
- A ACSERPRO valida o pedido e emite um certificado novo que corresponde à nova chave pública da AR;

- Certificado de AR novo é entregue a AR junto com a novo certificado da ACSERPRO;

Todos os certificados de usuário emitido pela ACSERPRO são revogados:

- São identificados todos os certificados ativos emitidos pela ACSERPRO comprometida;
- A AR submete um pedido de revogação para cada certificado ativo;
- A ACSERPRO processa a revogação e publica uma LCR imediatamente (por razões de desempenho a LCR é publicado somente após um certo volume de revogações);

Os usuários são notificados e emitem certificados novos:

- Os usuários são notificados que seus certificados foram revogados e são instruídos a solicitar um certificado novo (devem ser capturadas informações de contato de usuário durante sua inscrição);
- Cada usuário submete um pedido para um certificado novo;
- AR valida cada pedido segundo o procedimento padrão de validação (de acordo com a DPC) e submete pedidos válidos à ACSERPRO;
- A ACSERPRO processa cada pedido válido e gera um certificado;
- Usuário carrega o certificado junto com a chave pública e certificado da AC emissora.

Certificado da AR é revogado:

- Um pedido de revogação é feito à ACSERPRO para revogar;
- A ACSERPRO processa o pedido de revogação e imediatamente publica uma nova LCR;

A AR pede um certificado novo:

- Uma chave de AR nova é gerada e o pedido de certificado transmitido à ACSERPRO;
- A ACSERPRO processa o pedido e emite um certificado para a AR.

A ACSERPRO possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que a chave privada de uma entidade é comprometida, e que podem ser resumidas nas ações listadas a seguir.

- ✓ O instante do comprometimento é determinado. O instante de comprometimento é crítico para invalidar transações executadas depois daquele instante.
- ✓ O certificado de AC é revogado.
 - A AC Raiz é informada por comunicações seguras;
 - A revogação é processada com a data correta e instante do comprometimento;
 - A AC Raiz publica uma nova LCR imediatamente;
 - São notificados os titulares e usuários de certificado do comprometimento;
- ✓ ACSERPRO pede um novo certificado de AC à Raiz
 - A ACSERPRO revoga os certificados de AR antigos;

- Um novo par de chaves é gerado e a chave pública é entregue de maneira segura à AC Raiz para certificação;
- A AC Raiz valida o pedido de certificado e emite um novo certificado de AC;
- Procedimentos de *backup* de chaves privadas são executados;
- ✓ Emitem-se novos certificados de AR
 - Cada AR submete um pedido para um certificado novo;
 - A ACSERPRO valida o pedido e emite um certificado novo que corresponde à nova chave pública da AR;

- certificado de AR novo é entregue a AR junto com a nova chave pública e certificado da ACSERPRO;
- ✓ Todos os certificados de usuário emitido pela ACSERPRO comprometida são revogados
 - São identificados todos os certificados ativos emitidos pela ACSERPRO comprometida;
 - A AR submete um pedido de revogação para cada certificado ativo;
 - A ACSERPRO processa a revogação e publica uma LCR imediatamente;
- ✓ Os usuários são notificados e emitem certificados novos
 - Os usuários são notificados que seus certificados foram revogados e são instruídos a solicitar um certificado novo;
 - Cada usuário submete um pedido para um certificado novo;
 - AR valida cada pedido segundo o procedimento padrão de validação (de acordo com a DPC) e submete pedidos válidos à ACSERPRO;
 - A ACSERPRO processa cada pedido válido e gera um certificado;
 - Usuário carrega o certificado junto com o certificado da ACSERPRO emissora.

As ações seguintes são tomadas quando uma chave privada de AR é comprometida:

- ✓ O instante do comprometimento é determinado;
- ✓ O certificado de AR é revogado
 - Um pedido de revogação é feito à ACSERPRO para revogar o certificado que corresponde às chaves comprometidas. São providos a data e instante do comprometimento no pedido;
 - A ACSERPRO processa o pedido de revogação e imediatamente publica uma nova LCR;
- ✓ A AR pede um novo certificado
 - Uma chave de AR nova é gerada e o pedido de certificado transmitido à AC;
 - A ACSERPRO processa o pedido e emite um certificado para a AR;
- ✓ Todos os certificados de usuário emitidos/autorizados pelas chaves comprometidas são revogados
 - A AR examina os registros para identificar todos os pedidos de certificado processados depois que a chave for comprometida;
 - Um pedido de revogação é feito à ACSERPRO para esses certificados de usuário;
 - São notificados os proprietários de certificado da revogação de seus certificados.

A ACSERPRO possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso de desastre natural ou de outra natureza. O propósito deste plano é restabelecer as principais operações da ACSERPRO quando a operação de sistemas é significativamente e adversamente abalada por fogo, greves, etc.

O plano garante que qualquer impacto em operações de sistema não causará um impacto operacional direto e imediato dentro da ICP-Brasil da qual a ACSERPRO ou AR faz parte. Isto significa que o plano deve ter como meta primária, restabelecer a ACSERPRO ou plataforma de AR para tornar acessível os registros lógicos

mantidos dentro do *software*. Devem ser tomadas às ações de recuperação aprovadas dentro do plano segundo uma ordem de prioridade.

6.22. Extinção da ACSERPRO

Quando for necessário terminar o serviço da ACSERPRO, o impacto do término deve ser minimizado da melhor forma possível tendo em vista as circunstâncias prevaletentes. Isto inclui:

- ✓ Prover com maior antecedência possível notificação para:
 - a AC Raiz da ICP-Brasil;
 - todas as entidades subordinadas;
 - A transferência progressiva do serviço, e registros operacionais, para um sucessor da ACSERPRO, que deverá observar os mesmos requisitos de segurança exigidos para a ACSERPRO extinta;
- ✓ Preservar qualquer registro não transferido a um sucessor da ACSERPRO.

No caso de término programado, a ACSERPRO deve proporcionar para as AR vinculadas notificação com um mínimo de oito semanas de antecedência dos desligamentos propostos e de qualquer arranjo que foi feito ou será feito para a continuidade de serviços por um sucessor da ACSERPRO. As AR vinculadas devem notificar os Titulares de Certificado prontamente, e informar sobre a transferência progressiva de chaves novas e certificados para um sucessor da ACSERPRO.

No caso de um desligamento de emergência da ACSERPRO, por exemplo devido ao comprometimento da chave privada da ACSERPRO, a ACSERPRO proverá às AR vinculadas com tanta notificação quanto é prático e razoável nas circunstâncias prevaletentes. Todas as chaves e certificados serão revogados imediatamente pela ACSERPRO antes da parada de emergência. Os serviços de certificação devem ser recomeçados pela mesma ACSERPRO ou uma sua sucessora tão logo quanto possível depois da desativação ter sido efetuada.

No evento em que é necessário terminar a ACSERPRO todos os certificados de Titular de Certificado subordinados são revogados antes da paralisação ou transferidos a uma ACSERPRO substituta.

Onde praticável, deve ser planejada a revogação de certificados para coincidir com a transferência progressiva para uma ACSERPRO sucessora. Compensação ou restituição para Titulares de Certificados pela revogação dos certificados antes da data de expiração é uma questão contratual.

As PC sob as quais a sucessora da ACSERPRO emite certificados é uma questão contratual entre os participantes e está fora da extensão da DPC. Porém, tais PC devem ter sido também aprovadas pelo CG da ICPBrasil para assegurar conformidade com esta DPC na extensão do que é prático e razoável:

- A ACSERPRO sucessora deve assumir os mesmos direitos, obrigações e deveres como a ACSERPRO em desativação;
- As PC da ACSERPRO sucessora devem impor as mesmas exigências e deve conferir os mesmos benefícios como as PC sob as quais a ACSERPRO terminada emitiu certificados.
- A ACSERPRO sucessora deve emitir novos certificados a todas AR, e Titulares de Certificado subordinados cujos certificados foram revogados pela ACSERPRO terminada, após as AR e Titulares de Certificado terem feito uma nova solicitação de certificado, satisfazendo as exigências das novas PC implementadas pela ACSERPRO sucessora.

6.23. Identificação e Autenticação

No domínio da ACSERPRO, o atributo sujeito nos certificados emitidos para Titulares de Certificado são do tipo *Distinguished Name*, contendo sempre o seu nome no formato previsto padrão ITU X.500.

Nomes distintos devem possuir algum significado. Podem ser utilizados pseudônimos no componente de nome comum de um nome distinto caso solicitado por um Titular de Certificado, contanto que o mesmo possa provar satisfatoriamente que possui o direito de usar o pseudônimo. As AR não devem aceitar pseudônimos que acreditem poder causar ofensa. A ACSERPRO suporta o uso de certificados como uma forma de identificação dentro de uma comunidade de interesses particular. Certificados anônimos não são emitidos pela ACSERPRO.

Os procedimentos normais em alguns tipos de geração de certificado requerem a inserção de um nome de organização e departamento como parte do nome distinto.

Nomes distintos devem ser únicos e não ambíguos. Números ou letras adicionais poderão ser incluídos ao nome de cada entidade para assegurar a unicidade do campo.

A ACSERPRO se reserva o direito de tomar todas as decisões na hipótese de haver disputa decorrente da igualdade de nomes entre solicitantes de

certificados. Durante o processo de confirmação de identidade, caberá ao solicitante do certificado provar o seu direito de uso de um nome específico.

Não existe, no âmbito da ACSERPRO, processos de tratamento, reconhecimento e confirmação de autenticidade de marcas registradas.

O sistema de certificação, implementado e utilizado pela ACSERPRO no gerenciamento do ciclo de vida de seus certificados, controla e garante, de forma automática, a entrega do certificado somente ao detentor da chave privada correspondente à chave pública constante do certificado. A mensagem de solicitação de certificado obedece ao formato PKCS#10, que inclui, na própria mensagem, a assinatura digital da mesma, realizada com a chave privada correspondente à chave pública contida

na solicitação. Ao recebê-la o *software* de certificação (SGC) procede a verificação automática da assinatura digital com uso da chave pública incluída nessa solicitação. Esse

teste confirma a posse da chave privada pelo requisitante. A solicitação é então armazenada no banco de dados do SGC e possui, associado, um número de referência. Este número é impresso no Termo de Responsabilidade junto com os dados da entidade solicitante. Os dados são autenticados pela AR através de documentos oficiais, efetivando a vinculação da solicitação e chave privada à entidade autenticada pela AR.

A autenticação da Identidade de uma Organização não se aplica aos certificados emitidos pela ACSERPRO. Já a confirmação da identidade de um indivíduo deverá ser realizada mediante a presença física do interessado, com base em documentos de identificação legalmente aceitos, com base na ICP-Brasil.

Os Titulares de Certificado serão comunicados da necessidade da renovação com uma antecedência mínima de um mês pela ACSERPRO. As solicitações de renovação de certificados devem ser feitas pelos próprios Titulares de Certificado quando do recebimento dessa notificação, solicitando por meio eletrônico, assinada digitalmente com o uso de certificado vigente de mesmo tipo, podendo repetir esse procedimento por 2 (duas) ocorrências sucessivas. Para o certificado de equipamento e aplicações não há o processo de renovação.

Para o caso específico de revogação de um certificado de titular pela ACSERPRO, após a revogação de seu certificado o titular do certificado deverá executar os processos regulares de geração de seu novo par de chaves.

6.24. Operações sobre certificados

Os requisitos e procedimentos mínimos necessários para a aceitação de uma solicitação de emissão de certificado devem ser:

- A comprovação de atributos de identificação constantes do certificado;
- Um contrato assinado, que estabeleça termos e condições aplicados ao uso do certificado.

As AR devem tomar os cuidados necessários ao aceitar e processar solicitações de certificado. Um certificado será considerado válido a partir do momento de sua emissão.

O recebimento de um certificado pelo Titular de Certificado e o uso subsequente das chaves e certificado, constitui aceitação do certificado por parte do Titular de Certificado. No caso de certificados de equipamentos, aplicações ou pessoas jurídicas, a aceitação é feita pela pessoa responsável pelo uso subsequente ao recebimento do certificado.

A revogação pode ser descrita como a permanente inutilização de um certificado. Um certificado de AR ou de Titular de Certificado, é revogado tipicamente quando:

- ✓ As chaves foram comprometidas ou há suspeita de comprometimento por:
 - roubo, perda, revelação ou modificação da chave privada;
 - comprometimento da mídia armazenadora;
- ✓ Existe abuso deliberado de chaves e certificados, ou uma desobediência significativa de exigências operacionais;
- ✓ Um Titular de Certificado deixa a comunidade de interesses da PC sob a qual foi emitido, por exemplo:
 - um Titular de Certificado organizacional deixa o emprego ;
 - uma PC ou uma AR cessa sua operação;
 - ocorre o falecimento de um Titular de Certificado;
- ✓ Há uma emissão imprópria ou defeituosa de um certificado devido a:
 - um pré-requisito para a emissão do certificado que não foi satisfeito;
 - descoberta de uma evidência objetiva no certificado que leva a acreditar como sendo falso o certificado;
 - erro na entrada de dados ou outros erros de processamento;
- ✓ Uma informação do certificado torna-se inexata, por exemplo quando o Titular de Certificado muda o nome;
- ✓ Um pedido corretamente formatado é recebido do Órgão empregador do Titular do Certificado;
- ✓ Um pedido validado é recebido de um terceiro autorizado, por exemplo, uma determinação judicial;
- ✓ Um pedido feito por uma pessoa com procuração do Titular do Certificado; Certificado da ACSERPRO ou da AC Raiz da ICP-Brasil é revogado;
- ✓ Certificado de uma AR é revogado após comprovação da má utilização deste certificado;

Revogações de certificado podem ser iniciadas tipicamente por:

- Solicitação do Titular do Certificado;
- Solicitação do responsável pelo certificado, no caso de certificado de equipamentos, aplicações e pessoas jurídicas;
- Solicitação de empresa ou órgão (Dono de Certificado), quando o titular do certificado for seu empregado, funcionário ou servidor;
- Pela ACSERPRO;

- Por uma AR vinculada; ou
- Por determinação do CG da ICP-Brasil ou da AC Raiz.

As AR não podem revogar ou pedir a revogação de seus próprios certificados sob qualquer condição diferente das descritas na (DPC) Declaração de Práticas Certificadoras.

As práticas envolvidas no processo de um pedido de revogação variam, dependendo da identidade do solicitante. Como diretrizes gerais, fica estabelecido que:

- O solicitante da revogação de um certificado será identificado;
- As solicitações de revogação, bem como as ações delas decorrentes serão registradas e armazenadas;
- As justificativas para a revogação de um certificado serão documentadas;
- O processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado. O prazo limite para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação, está definido nas PC implementadas pela ACSERPRO.

As PC implementadas pela ACSERPRO estabelecem os prazos para a aceitação do certificado solicitado por seu titular, dentro dos quais a revogação do certificado poderá ser solicitada sem cobrança de tarifa pela ACSERPRO.

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da ACSERPRO.

A frequência de emissão das LCR será definida em cada PC implementada pela ACSERPRO, levando em conta sempre os prazos mínimos estabelecidos pelo CG da ICP-Brasil.

Os números de série de certificados de qualquer entidade final que estejam revogados aparecem na LCR emitida pela ACSERPRO. Estes números permanecem nas LCR emitidas até a data de expiração dos certificados ser atingida, sendo removidos na primeira LCR emitida após data de suas expirações. São emitidas LCR nas frequências determinadas nas PC, mesmo quando não houver nenhuma mudança ou atualização, para assegurar a periodicidade da informação. Não são emitidos certificados de AC pela ACSERPRO, portanto não são emitidas LCR correspondentes.

Todos os certificados revogados no domínio da ACSERPRO são listados na LCR que pode ser acessada no endereço *Web* contido no próprio certificado. Antes de aceitar um certificado os Titulares de Certificados devem verificar a situação do mesmo na LCR corrente. Se for utilizada uma cópia local da LCR, esta deve ser atualizada se estiver expirada. Também deve ser verificada a autenticidade da LCR por meio das verificações de assinatura e do seu período de validade.

A ACSERPRO poderá disponibilizar recursos para revogação *on-line* de certificados, quando definido em sua PC, ou para verificação *on-line* de estado de

certificados. A verificação da situação de um certificado poderá ser feita diretamente na ACSERPRO, por meio do protocolo OCSP (*On-line Certificate Status Protocol*).

A ACSERPRO proverá, quando determinado na sua respectiva PC, diretório *on-line* ou um servidor de OCSP para verificar o estado dos certificados emitidos pela ACSERPRO.

Quando houver comprometimento ou suspeita de comprometimento da chave privada, o Titular do Certificado deverá comunicar imediatamente a ACSERPRO. Os requisitos específicos aplicáveis a revogação do certificado nestas circunstâncias são descritos nas PC implementadas pela ACSERPRO. Os meios utilizados para comunicar um comprometimento ou suspeita de comprometimento de chave são descritos nas PC.

7. Conclusão

O uso da assinatura eletrônica tornou-se legal no país através da Medida Provisória 2.200, como já foi anteriormente citado, com força de Lei, que já esta na sua segunda reedição, esta de 24/08/2001. A MP regulamenta o uso da ICP-Brasil e do seu órgão gestor, dentre outros aspectos relevantes. Há uma serie de decretos que complementam e acompanham essa MP.

O Congresso Nacional esta discutindo o substitutivo que altera a MP 4.906, já aprovado por Comissão Especial da Câmara dos Deputados e aguardando votação em plenário. Esse substitutivo mantém a ICP-Brasil, mas legisla sobre inúmeros outros temas, como direitos do contribuinte, etc. E importante lembrar que, ate a aprovação desse substitutivo, a MP tem força de Lei e os atos, praticados sob sua égide, validade legal.

Além disso o seu artigo 10.o, parágrafo segundo, estabelece que qualquer forma de assinatura eletrônica que seja pactuada entre as partes tem também validade legal para elas (isto não vale para o governo federal, obrigado a usar a ICP-Brasil). E com base nesse dispositivo que alguns bancos comerciais vem implementando sistemas de assinatura eletrônica, utilizando senhas ou mesmo certificados digitais, embora sem a necessária certificação pela Autoridade Certificadora-Raiz brasileira.

Quanto a confiança que os executivos brasileiros depositam na ICP-Brasil, mais da metade dos executivos presentes ao Fórum de Certificação Digital do Security Week – Brasil – 2002, realizado em São Paulo, em março último, confia na ICP-Brasil. O Serpro foi co-anfitrião do ICP-Forum, que continha uma grade temática especifica sobre Estratégias de Autenticação e Certificação Digital.

O Security Week – Brasil 2002, realizado de 25 a 27 de marco, foi o maior evento especifico sobre segurança da informação já realizado no país, que reuniu empresas e profissionais especializados. Cerca de 1500 pessoas participaram de fóruns, seminários, workshops e debateram sobre o tema de “Conferencia Internacional da Gestão da Segurança da Informação”.

Durante todo o evento foram realizadas diversas enquetes aplicadas a um grupo total de 600 executivos e no Talkshow do ICP-Forum. Os resultados apurados indicam que 89% dos presentes confiam total ou parcialmente na ICP-Brasil, o que demonstra o elevado grau de confiança dos executivos na capacidade tecnológica do Governo Federal.

Ao mesmo tempo, estes mesmos executivos, quase que unanimemente, reconhecem a importância que a certificação digital terá para o seu negócio, com 47% dos presentes declarando entender ser vital e 51% considerando, no mínimo, importante.

No mesmo Talkshow, foi perguntado para os presentes qual deveria ser o grande disseminador da utilização de certificação digital pelo mercado, e 49% optaram pelas Transações Financeiras, enquanto 26% e 25% escolheram o imposto de renda e eleições eletrônicas, respectivamente.

8. Referências

[Dias, Cláudia, 2000] – Dias, Cláudia. “Segurança e Auditoria da Tecnologia da Informação”. Axcel Books do Brasil, 2000.

Tema, a revista do Serpro - Ano XXVI n°s 157, 159 e edição comemorativa.

Autoridade Certificadora para Acesso Seguro – Martins, Alessandro. Laboratório RAVEL/COPPE/UFRJ.

Declaração de Práticas de Certificação da Autoridade Certificadora do Serpro.