	SERVIÇO PÚBLICO FEDERAL **MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA E COMÉRCIO EXTERIOR** **INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL** **PRESIDÊNCIA**

PRESIDÊNCIA	**29/07/2013**
RESOLUÇÃO	**Nº 103/2013**

Assunto: Estabelece normas para utilização do Certificado Digital do Tipo A3 no Instituto Nacional da Propriedade Industrial – INPI.

O PRESIDENTE e a COORDENADORA-GERAL DE TECNOLOGIA DA INFORMAÇÃO do INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL – INPI, nos exercícios de suas atribuições regimentais, e

CONSIDERANDO o disposto no art. 5º, inciso LXXVIII, da Constituição da República Federativa do Brasil de 1988, no qual são assegurados a todos, no âmbito judicial e administrativo, a razoável duração do processo e os meios que garantam a celeridade de sua tramitação;

CONSIDERANDO o Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

CONSIDERANDO a Medida Provisória nº 2.200-2, de 24 de agosto de 2001, que institui a Infraestrutura de Chaves Públicas Brasileiras – ICP-Brasil, e transforma o Instituto Nacional de Tecnologia da Informação em autarquia;

CONSIDERANDO, também, o Decreto nº 3.996, de 31 de outubro de 2001, o qual dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal;

CONSIDERANDO a necessidade de estabelecer procedimentos para a devida utilização dos certificados digitais no âmbito do INPI;

CONSIDERANDO a atual política do INPI, a qual trata da redução da utilização de papel indo ao encontro dos norteadores da Agenda Ambiental da Administração Pública – A3P;

CONSIDERANDO a busca por maior eficiência, eficácia e transparência do serviço público;

CONSIDERANDO o estabelecido no Plano Diretor de Tecnologia da Informação – PDTI; a evolução tecnológica constante onde as ferramentas eletrônicas permitem a publicidade dos atos administrativos na rede mundial de computadores com a devida segurança e celeridade por meio da aplicação de novas tecnologias; e a estratégia de modernização do Instituto, no qual se inclui a Gestão da Segurança da Informação com o fito de melhorar a qualidade do desempenho institucional junto à sociedade; e

CONSIDERANDO, por último, a necessidade de regulamentar os certificados digitais fornecidos pelo INPI,

RESOLVEM:

Art. 1° Para efeitos desta Norma, são estabelecidos os seguintes conceitos e definições:

I. **Assinatura digital:** código anexado ou logicamente associado a uma mensagem eletrônica que permite de forma única e exclusiva a comprovação da autoria de um determinado conjunto de dados (um arquivo, um e-mail ou uma transação). A assinatura digital comprova que a pessoa (relacionada ao CPF) criou ou concorda com um documento assinado digitalmente, como a assinatura de próprio punho comprova a autoria de um documento escrito. A verificação da origem do dado é feita com a chave pública do remetente;

II. **Autenticidade:** qualidade de um documento ser o que diz ser, independente de se tratar de minuta, original ou cópia e que é livre de adulterações ou qualquer outro tipo de corrupção;

III. **Autoridade Certificadora (AC):** entidade que emite, renova ou revoga certificados digitais de outras ACs ou de titulares finais;

IV. **Autoridade Certificadora Raiz (AC Raiz):** entidade que credencia, audita e fiscaliza as demais entidades da ICP-Brasil. Assina seu próprio certificado e os certificados das ACs imediatamente abaixo dela. É também a Entidade de Auditoria do tempo da Rede de Carimbo do Tempo da ICP-Brasil;

V. **Autoridade de Registro (AR):** entidade responsável pela interface entre o usuário e a Autoridade Certificadora. Vinculada a uma AC que tem por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais às AC e identificação, de forma presencial, de seus solicitantes. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota;

VI. **Certificação Digital:** atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação. Esse reconhecimento é inserido em um Certificado Digital, por uma Autoridade Certificadora;

VII. **Certificado de Assinatura Digital:** são os certificados usados para confirmação da identidade na *web*, correio eletrônico, transações *on-line*, redes privadas virtuais, transações eletrônicas, informações eletrônicas, cifração de chaves de sessão e assinatura de documentos com verificação da integridade de suas informações;

VIII. **Certificado digital:** conjunto de dados de computador, gerados por uma Autoridade Certificadora, em observância à Recomendação Internacional ITU-T X.509, que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação;

IX. **Certificado do tipo A3:** certificado em que a geração e o armazenamento das chaves criptográficas são feitos em cartão Inteligente ou *token*, ambos com capacidade de geração de chaves e protegidos por senha, ou hardware criptográfico aprovado pela ICP-Brasil. A validade máxima do certificado é de 03 (três) anos;

X. **Certificado Expirado:** certificado cuja data de validade foi ultrapassada;

XI. **Certificado Válido:** certificado dentro do prazo de validade, que não tenha sido revogado e que seja possível validar toda a cadeia do certificado até uma AC Raiz;

XII. **Chave Privada:** chave secreta do par de chaves criptográficas em um sistema de criptografia assimétrica. É mantida secreta pelo seu dono (detentor de um certificado digital) e usada para criar assinaturas digitais e para decifrar mensagens ou arquivos cifrados com a chave pública correspondente;

XIII. **Chave Pública:** chave mantida pública em um sistema de criptografia assimétrica. É divulgada pelo seu dono e usada para verificar a assinatura digital criada com a chave privada correspondente. Dependendo do algoritmo, a chave pública também é usada para cifrar mensagens ou arquivos que possam, então, ser decifrados com a chave privada correspondente;

XIV. **Integridade:** garantia oferecida ao usuário de que documento eletrônico, mensagem ou conjunto de dados não foi alterada, nem intencionalmente, nem acidentalmente por pessoas não autorizadas durante sua transferência entre sistemas ou computadores;

XV. **Par de Chaves:** chaves privada e pública de um sistema criptográfico assimétrico. A chave privada e sua chave pública são matematicamente relacionadas e possuem certas propriedades, entre elas a de que é impossível a dedução da chave privada a partir da chave pública conhecida. A chave pública pode ser usada para verificação de uma assinatura digital que a chave privada correspondente tenha criado ou a chave privada pode decifrar a uma mensagem cifrada a partir da sua correspondente chave pública. A chave privada deve ser de conhecimento exclusivo do titular do certificado;

XVI. ***PIN (Personal Identification Number)*:** sequência de números e/ou letras (senha) usadas para liberar o acesso à chave privada, ou outros dados armazenados na mídia, somente para pessoas autorizadas;

XVII. ***PUK (Personal Identification Number Unblocking Key)*:** chave para desbloqueio do número de identificação pessoal (PIN), o qual normalmente fica bloqueado após várias tentativas inválidas. Como o PIN, a senha PUK deve ser guardada de forma segura, pois ambas permitem, em dispositivos como *tokens* e smart cards, o acesso à chave privada de um titular de certificado;

XVIII. **Senha:** conjunto de caracteres, conhecidos apenas pelo usuário, que fornecem acesso ao arquivo, computador ou programa. Senhas são geralmente usadas em conjunto com o nome do usuário que o autentica e o garante autorização ao acesso;

XIX. **Senha Fraca ou Óbvia:** é aquela onde se utilizam caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequena, tal como: datas de aniversário, casamento, nascimento, o próprio nome, o nome de familiares, sequências numéricas simples, palavras com significado, dentre outras;

XX. **Titular do Certificado:** entidades, pessoa física ou jurídica, para as quais foram emitidos um certificado digital. O assinante é o titular da chave privada correspondente à chave pública contida no certificado e possui a capacidade de utilizar tanto uma quanto a outra;

XXI. ***Token*:** dispositivo para armazenamento do Certificado Digital de forma segura, sendo seu funcionamento parecido com o smart card, tendo sua conexão com o computador via USB;

XXII. **Usuário:** pessoa que utiliza certificado digital apresentado por um titular;

XXIII. **Usuário Final:** pessoa física ou jurídica que possui um certificado digital. Sinônimo de Titular de Certificado;

XXIV. **Validade do Certificado:** período de tempo em que o certificado está com sua data de validade operacional;

XXV. **Verificação da Validade do Certificado:** processo realizado por um destinatário ou terceira parte para confirmar que o certificado de um titular, usuário final, é válido e era operacional na data e hora que uma assinatura digital pertinente foi criada;

XXVI. **Verificação de Assinatura Digital:** ação realizada para determinar com precisão que a assinatura digital foi criada durante o período operacional de um certificado válido por uma chave privada correspondente à chave pública contida no certificado e que a mensagem associada não tenha sido alterada desde que a assinatura digital foi criada.

Art. 2° Os certificados digitais do tipo A3 utiliz ados pelo INPI e fornecidos por pessoa jurídica (Autoridade Certificadora/Autoridade de Registro) devidamente contratada com base nas legislações e normas em vigor para prestação de serviços de certificação digital, bem como devidamente habilitada/credenciada pela Autoridade Certificadora Raiz (ITI), destinam-se aos agentes públicos.

Art. 3º Os certificados de assinatura digital são de uso pessoal e intransferível devendo, o titular do certificado, zelar pela não divulgação das senhas PIN e/ou PUK, bem como pelo dispositivo que contém as chaves pública e privada (*token*), sob pena de responsabilidade civil, penal e administrativa.

Art. 4º O certificado digital funcionará como uma identidade virtual, na qual será permitida a identificação segura e inequívoca do autor de uma mensagem (*e-mail*), da realização de transações feitas em meios eletrônicos, como a *web*, por exemplo, bem como para a utilização nos softwares internos e de uso próprio do INPI.

Art. 5º Aos que necessitarem, em função do exercício da função pública, será fornecido um certificado digital do tipo A3 desde que a solicitação, devidamente justificada, seja autorizada pela Coordenação da área ou, na impossibilidade desta, por Autoridade imediatamente superior.

Art. 6º O certificado digital e o respectivo suporte criptográfico (token) serão concedidos gratuitamente aos usuários que necessitarem utilizar a assinatura digital em razão do cargo público ou da função gratificada para a qual forem designados.

Art. 7º Nos sistemas utilizados no INPI, a certificação digital confere aos documentos assinados digitalmente o mesmo valor jurídico e/ou administrativo dos documentos em papel assinados de próprio punho.

Art. 8º A utilização do Certificado Digital permite a segurança dos usuários em função das seguintes características:

I. **Autenticidade**: assegura a identificação do autor do documento eletrônico ou do autenticador do documento reproduzido em meio eletrônico, assinado digitalmente;
II. **Confidencialidade**: garantia de que somente as pessoas envolvidas no processo terão acesso às informações transmitidas de forma eletrônica pela rede;
III. **Identidade**: garantia de que o emissor de uma mensagem ou pessoa que executou determinada transação de forma eletrônica não poderá negar sua autoria;
IV. **Irretratabilidade**: impossibilita ao usuário negar a autenticidade do documento após esse ter sido devidamente assinado digitalmente; e
V. **Integridade**: garantia de que a assinatura digital não mais corresponderá ao documento quando da realização de qualquer alteração/modificação no conteúdo deste.

Art. 9° O usuário fica obrigado a utilizar seu pró prio Certificado Digital para poder praticar atos assinados digitalmente.

§ 1º O portador é responsável civil, criminal e administrativamente pelos atos praticados.

§ 2° A utilização do certificado digital em sistemas fora do âmbito do Instituto Nacional da Propriedade Industrial é de inteira responsabilidade do seu portador.

Art. 10 É imputado, ao usuário, o ressarcimento do valor quando:

I. Inviabilizar o certificado após exceder, sem sucesso de acesso à senha, por três tentativas de PIN e/ou por três tentativas de PUK, bem como por exceder o número de tentativas em decorrência do tipo de mídia relativa ao certificado;

II. Ocorrer perda ou dano irreparável do token e do certificado digital.

§ 1º Somente não haverá ressarcimento em caso de roubo ou furto, no qual o usuário deverá apresentar o Boletim de Ocorrência Policial à Coordenação-Geral de Tecnologia da Informação (CGTI) de forma a proceder à revogação do certificado.

§ 2º O valor, a ser ressarcido pelo usuário, será o do estabelecido em contrato, considerando-se os possíveis termos aditivos ou apostilamentos.

Art. 11 Em caso de desligamento do usuário dos quadros do INPI, por qualquer motivo, o portador deverá remeter o token, ou equivalente, à CGTI para adoção das devidas providências.

Art. 12 Compete à Coordenação-Geral de Tecnologia da Informação, em especial:

I. Adotar as medidas cabíveis quanto à gestão de uso dos certificados digitais, compreendida a emissão, renovação e distribuição de certificados digitais, bem como a obrigação da revogação conforme estabelecido no parágrafo único do art. 10;

II. Adequar a infraestrutura de Tecnologia da Informação para uso dos certificados digitais;

III. Elaborar e divulgar padrões de compatibilidade dos certificados digitais e dos respectivos suportes criptográficos utilizados no INPI;

IV. Prover solução de Tecnologia da Informação para autorizar a troca de informações, por meio eletrônico, entre o INPI e outros órgãos ou demais entidades, com a utilização de certificado digital;

V. Desenvolver novas aplicações ou atualizar as existentes que requeiram a utilização de certificados digitais; e

VI. Registrar e controlar os certificados e respectivos suportes criptográficos de que trata o art. 6º.

Art. 13 No procedimento eletrônico observar-se-ão todas as regras processuais inerentes aos atos praticados.

Art. 14 Os casos omissos serão resolvidos pelo Presidente do Instituto Nacional da Propriedade Industrial.

Art. 15 Esta Resolução entra em vigor na data de sua publicação.

JORGE DE PAULA COSTA ÁVILA
Presidente

NEUSA MANSOUR
Coordenadora-Geral de Tecnologia da Informação