MERCOSUR/GMC EXT./RES. Nº 37/06

RECONHECIMENTO DA EFICÁCIA JURÍDICA DO DOCUMENTO ELETRÔNICO, A ASSINATURA ELETRÔNICA E A ASSINATURA ELETRÔNICA AVANÇADA NO ÂMBITO DO MERCOSUL

TENDO EM VISTA: O Tratado de Assunção, o Protocolo de Ouro Preto, o Protocolo de Olivos e as Decisões Nº 04/91 e 59/00 do Conselho do Mercado Comum e a Resolução Nº 24/03 do Grupo Mercado Comum.

CONSIDERANDO:

Que o desenvolvimento contínuo das tecnologias da informação e comunicação estão a serviço da consolidação e do desenvolvimento de uma sociedade da informação inclusiva, que promova o melhor aproveitamento socioeconômico dos bens imateriais.

Que o desenvolvimento das relações sociais e o estreitamento dos laços entre os cidadãos e as administrações dos Estados Partes, e destes entre si, dependem de medidas que garantam a segurança e a confiança nos documentos eletrônicos.

Que, para a segurança e a confiança nos documentos eletrônicos, se requerem assinaturas eletrônicas e serviços conexos.

Que as assinaturas eletrônicas avançadas, baseadas em um certificado reconhecido, permitem lograr maior nível de segurança.

Que devido à assimetria nos sistemas jurídicos nacionais sobre a matéria, é necessário adotar normas comuns, de acordo com os padrões internacionais a fim de promover um entendimento tecnológico entre as respectivas estruturas legais e técnicas dos Estados Partes.

Que o desenvolvimento da assinatura eletrônica avançada nos Estados Partes não restringirá as atividades relacionadas à emissão de certificados digitais vinculados a assinaturas eletrônicas, que terão seus efeitos jurídicos limitados à autonomia da vontade das partes que confiam nessas tecnologias ou não se opõem a sua utilização.

O GRUPO MERCADO COMUM
RESOLVE:

Art. 1- Âmbito de aplicação

A presente Resolução tem por finalidade reconhecer, nas condições previstas na presente norma, a eficácia jurídica dos documentos eletrônicos, da assinatura eletrônica e da assinatura eletrônica avançada no âmbito do MERCOSUL, contribuindo para sua utilização.

A presente norma não regula outros aspectos relacionados com a celebração e a validade dos atos jurídicos quando existirem requisitos de forma estabelecidos nas legislações nacionais, nem afeta as normas e limites contidos nas legislações nacionais que regulam o uso de documentos.

A presente norma não habilita a livre circulação de serviços de certificação digital no âmbito do MERCOSUL. No que diz respeito à prestação de serviços de certificação digital, os Estados Partes observarão as disciplinas estabelecidas no Protocolo de Montevidéu sobre o Comércio de Serviços do MERCOSUL e em suas listas de compromissos específicos.

Art. 2- Princípios

Os Estados Partes observarão os seguintes princípios:

1. Autonomia operativa e coordenação permanente entre as Infra-estruturas nacionais;
2. Interoperabilidade baseada em padrões internacionais;
3. Intercâmbio de informação e documentação digital entre os Estados Partes em condições técnicas seguras, com validade legal e valor probatório;
4. Transparência na gestão da certificação digital;
5. Tratamento neutro nas leis nacionais com relação às diversas tecnologias utilizadas nas atividades previstas na presente Resolução, de modo que permita a adaptação ao ritmo de desenvolvimento tecnológico inerente a essas atividades (neutralidade tecnológica);
6. Interpretação funcional dos termos e conceitos, a fim de assegurar que não sejam negados efeitos jurídicos a um processo ou tecnologia utilizado por um Estado Parte, pelo razão exclusiva de que lhe é atribuída uma nomenclatura distinta da prevista na presente Resolução.

Art. 3. Definições

Para os fins da presente Resolução, entender-se-á por:

1) "**Assinatura eletrônica**": os dados em forma eletrônica anexos a outros dados eletrônicos ou associados de maneira lógica com eles, utilizados pelo signatário como meio de identificação;

2) "**Assinatura eletrônica avançada**": a assinatura eletrônica que cumpre os requisitos seguintes:

a) requerer informação de exclusivo conhecimento do signatário, permitindo sua identificação unívoca;

b) ser criada por meios que o signatário possa manter sob seu exclusivo controle;

c) ser suscetível de verificação por terceiros;

d) estar vinculada a esses dados de tal modo que qualquer alteração subseqüente nos mesmos seja detectável; e

e) haver sido criada utilizando um dispositivo de criação de assinatura tecnicamente seguro e confiável e estar baseada em um certificado reconhecido e válido no momento da assinatura.

3) **“Assinatura digital”:** utilizada indistintamente com “assinatura eletrônica avançada” para os fins da presente Resolução**.**

4) **“Signatário”:** a pessoa física ou jurídica que utiliza legalmente um dispositivo para a criação de uma assinatura eletrônica**;**

5) **“Documento eletrônico”:** representação digital de atos ou fatos, independentemente do suporte utilizado para sua fixação, armazenamento ou arquivo**.**

6) **“Documento digital”:** utilizada indistintamente com “documento eletrônico” para os fins da presente Resolução.

7) **“Certificado digital”**: documento eletrônico assinado digitalmente que vincula alguns dados de verificação de assinatura com seu titular e confirma sua identidade.

8) **“Certificado reconhecido”**: certificado digital emitido por um prestador de serviços acreditado que cumpre os requisitos estabelecidos pela legislação nacional.

9) **“Certificado avançado”:** utilizada indistintamente com “Certificado reconhecido” para os fins da presente Resolução**.**

10) **“Prestador de serviços de certificação”**: pessoa física ou jurídica, conforme a legislação nacional, que expede certificados ou presta outros serviços relacionados com a assinatura eletrônica.

Art. 4. Efeitos Legais dos Documentos Eletrônicos e das Assinaturas Eletrônicas

Os Estados Partes reconhecem que os documentos eletrônicos satisfazem os requisitos de escritura. Em virtude desse fato, em qualquer dos Estados Partes os documentos eletrônicos terão os mesmos efeitos jurídicos que os documentos escritos, salvo exceções contempladas nas legislações nacionais.

Os Estados Partes reconhecerão efeitos jurídicos à assinatura eletrônica quando esta for admitida como válida pelas partes que a utilizarem ou for aceita pela pessoa a quem for oposto o documento a ela vinculado.

Os Estados Partes assegurarão que não serão negados efeitos probatórios a um documento eletrônico pela razão exclusiva de que este não esteja vinculado a uma assinatura eletrônica avançada, se por algum meio inequívoco se puder demonstrar sua autenticidade e integridade.

Respeitar-se-á a liberdade das partes para concertar, de comum acordo, as condições em que aceitarão as assinaturas eletrônicas, conforme sua legislação nacional.

No caso de ser desconhecida a assinatura eletrônica por alguma das partes, compete à outra parte provar sua validade.

Art. 5- Assinatura eletrônica avançada: Reconhecimento Mútuo

Com o objetivo de alcançar o reconhecimento mútuo das assinaturas eletrônicas avançadas e dos certificados digitais, os Estados Partes poderão celebrar, entre si, acordos de reconhecimento mútuo. Para esse fim, o GMC aprovará as Diretrizes para a celebração desses acordos. Tais Diretrizes refletirão o estado da matéria no momento de sua aprovação e poderão ser atualizadas por proposta do SGT Nº 13, de maneira que acompanhe a evolução das tecnologias a elas relacionadas.

Mediante os Acordos de Reconhecimento Mútuo se outorgará às assinaturas eletrônicas avançadas que cumpram com as condições neles dispostas o mesmo valor jurídico e probatório atribuído às assinaturas manuscritas.

Os Estados Partes reconhecerão a autenticidade e a integridade de um documento eletrônico assinado com uma assinatura eletrônica avançada, admitindo-a como prova documental em processos judiciais, conforme se disponha nos Acordos de Reconhecimento Mútuo.

Os Estados Partes indicarão, no âmbito do SGT Nº 13, quais serão os organismos competentes habilitados para assinar Acordos de Reconhecimento Mútuo.

Art. 6 – Certificados Digitais Reconhecidos

Os Acordos de Reconhecimento Mútuo estabelecerão as condições sob as quais os certificados digitais expedidos em um Estado Parte desse Acordo terão a mesma validade jurídica nos demais Estados Partes que assinem o Acordo.

Estas condições deverão contemplar, pelo menos, que os certificados digitais:

a) sejam emitidos por um prestador de serviços de certificação sob o sistema nacional de credenciamento e controle previsto no artigo 7;

b) respondam a formatos padrão reconhecidos internacionalmente, determinados pela autoridade de aplicação de cada Estado Parte;

c) respondam aos critérios mínimos estabelecidos nas Diretrizes mencionadas no artigo 5; e

d) contenham, pelo menos, os dados que permitam:
   1. identificar indubitavelmente o titular e o prestador de serviços de certificação que o emitiu, indicando seu período de vigência e os dados que permitam sua identificação única;
   2. ser suscetível de verificação em relação a seu estado de revogação;
   3. diferenciar claramente a informação verificada da não verificada incluídas no certificado digital;
   4. contemplar a informação necessária para a verificação da assinatura;
   5. identificar a política de certificação sob a qual foi emitido.

Art. 7 – Prestação de Serviços de Certificação

Os Estados Partes não submeterão a credenciamento prévio a prestação de serviços de certificação, exceto aqueles vinculados a uma assinatura eletrônica avançada, em conformidade com os termos da presente Resolução.

Os Estados Partes assegurarão a criação de um sistema adequado de credenciamento e controle dos prestadores de serviços de certificação que emitam certificados reconhecidos que permitam a verificação de assinaturas eletrônicas avançadas, estabelecidos em seus respectivos territórios.

Os Estados Partes poderão submeter o uso da firma eletrônica e da firma eletrônica avançada no setor público a possíveis determinações adicionais. Tais determinações serão objetivas, transparentes, proporcionais e não no discriminatórias, e somente poderão fazer referência às características específicas da aplicação de que se trate. Estas determinações não deverão obstar os serviços transfronteiriços.

Art. 8 – Responsabilidades

Os Estados Partes assegurarão como mínimo que um prestador de serviços de certificação credenciado nos termos do artigo 7, seja responsável pelos danos e prejuízos causados a qualquer pessoa física ou jurídica que confie razoavelmente no certificado digital por ele emitido, no que respeite a:

a) a inclusão de todos os campos e dados requeridos pelas respectivas Infra-estruturas nacionais para o certificado reconhecido e a exatidão dos mesmos, no momento de sua emissão.

b) que no momento de emissão de um certificado reconhecido por parte do prestador de serviços de certificação credenciado, a assinatura nele identificada obedece aos dados de criação de assinatura correspondentes aos dados de verificação incluídos no certificado reconhecido do prestador, com o objetivo de assegurar a cadeia de confiança.

c) os erros ou omissões que apresentem os certificados reconhecidos que emitam, ou pela inobservância dos procedimentos de certificação estabelecidos a partir dos Acordos de Reconhecimento Mútuo.

d) o registro no tempo e na forma da revogação dos certificados reconhecidos que haja emitido, quando assim corresponder.

Corresponde ao prestador de serviços de certificação credenciado demonstrar que não atuou nem com culpa nem com dolo.

Os Estados Partes assegurarão que o prestador de serviços de certificação credenciado nos termos do artigo 7, possa indicar em um certificado reconhecido de forma identificável por terceiros, os limites de sua utilização.

O prestador de serviços de certificação credenciado nos termos do artigo 7, não será responsável pelos prejuízos resultantes da utilização de um certificado reconhecido pelo emitido, que exceda o alcance definido em sua Política de Certificação. Tampouco responderá por eventuais inexatidões no certificado reconhecido que resultem da informação verificada facilitada pelo titular, sempre que o prestador de serviços de certificação credenciado possa demonstrar que tenha cumprido todas as medidas previstas em suas políticas e procedimentos de certificação.

Art. 9- Proteção de Dados Pessoais

Os Estados Partes deverão prever que um prestador de serviços de certificação que emite certificados reconhecidos destinados ao público, somente possa coletar os dados pessoais diretamente da pessoa a quem esses dados se referem, depois de haver obtido

seu consentimento expresso e somente na medida em que os mesmos sejam necessários para a emissão e manutenção do certificado. Os dados não poderão ser obtidos ou utilizados para outro fim, sem o consentimento expresso do titular dos dados.

Os Estados Partes garantirão a confidencialidade dos demais dados pessoais requeridos para a emissão do certificado reconhecido e que não figurem nele, nos termos expostos pelo presente artigo.

Art. 10 – Incorporação

Os Estados Partes deverão incorporar a presente Resolução a seus ordenamentos jurídicos nacionais.

XXXI GMC EXT. – Córdoba, 18/VII/06