Decreto nº 3.587, de 05.09.2000
Anexo I
Anexo II

Estabelece normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal - ICP-Gov, e dá outras providências.

O PRESIDENTE DA REPÚBLICA, no uso das atribuições que lhe confere o art. 84, incisos IV e VI, da Constituição,

DECRETA:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º A Infra-Estrutura de Chaves Públicas do Poder Executivo Federal - ICP-Gov será instituída nos termos deste Decreto.

Art. 2º A tecnologia da ICP-Gov deverá utilizar criptografia assimétrica para relacionar um certificado digital a um indivíduo ou a uma entidade.

§ 1º A criptografia utilizará duas chaves matematicamente relacionadas, onde uma delas é pública e, a outra, privada, para criação de assinatura digital, com a qual será possível a realização de transações eletrônicas seguras e a troca de informações sensíveis e classificadas.

§ 2º A tecnologia de Chaves Públicas da ICP-Gov viabilizará, no âmbito dos órgãos e das entidades da Administração Pública Federal, a oferta de serviços de sigilo, a validade, a autenticidade e integridade de dados, a irrevogabilidade e irretratabilidade das transações eletrônicas e das aplicações de suporte que utilizem certificados digitais.

Art. 3º A ICP-Gov deverá contemplar, dentre outros, o conjunto de regras e políticas a serem definidas pela Autoridade de Gerência de Políticas - AGP, que visem estabelecer padrões técnicos, operacionais e de segurança para os vários processos das Autoridades Certificadoras - AC, integrantes da ICP-Gov.

Art. 4º Para garantir o cumprimento das regras da ICP-Gov, serão instituídos processos de auditoria, que verifiquem as relações entre os requisitos operacionais determinados pelas características dos certificados e os procedimentos operacionais adotados pelas autoridades dela integrantes.

Parágrafo único. Além dos padrões técnicos, operacionais e de segurança, a ICP-Gov definirá os tipos de certificados que podem ser gerados pelas AC.

CAPÍTULO II
DA ORGANIZAÇÃO DA ICP-Gov

Art. 5º A arquitetura da ICP-Gov encontra-se definida no Anexo I a este Decreto.

Art. 6º À Autoridade de Gerência de Políticas - AGP, integrante da ICP-Gov, compete:

I - propor a criação da Autoridade Certificadora Raiz - AC Raiz;

II - estabelecer e administrar as políticas a serem seguidas pelas AC;

III - aprovar acordo de certificação cruzada e mapeamento de políticas entre a ICP-Gov e outras ICP externas;

IV - estabelecer critérios para credenciamento das AC e das Autoridades de Registro - AR;

V - definir a periodicidade de auditoria nas AC e AR e as sanções pelo descumprimento de normas por ela estabelecidas;

VI - definir regras operacionais e normas relativas a:

a) Autoridade Certificadora - AC;
b) Autoridade de Registro - AR;
c) assinatura digital;
d) segurança criptográfica;
e) repositório de certificados;
f) revogação de certificados;
g) cópia de segurança e recuperação de chaves;
h) atualização automática de chaves;
i) histórico de chaves;
j) certificação cruzada;
l) suporte a sistema para garantia de irretratabilidade de transações ou de operações eletrônicas;
m) período de validade de certificado;
n) aplicações cliente;

VII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Gov, em especial da Política de Certificados - PC e das Práticas e Regras de Operação da Autoridade Certificadora, de modo a garantir:

a) atendimento às necessidades dos órgãos e das entidades da Administração Pública Federal;

b) conformidade com as políticas de segurança definidas pelo órgão executor da ICP-Gov; e

c) atualização tecnológica.

Art. 7º Para assegurar a manutenção do grau de confiança estabelecido para a ICP-Gov, as AC e AR deverão credenciar-se junto a AGP, de acordo com as normas e os critérios por esta autoridade estabelecidos.

Art. 8º Cabe à AC Raiz a emissão e manutenção dos certificados das AC de órgãos e entidades da Administração Pública Federal e das AC privadas credenciadas, bem como o gerenciamento da Lista de Certificados Revogados - LCR.

Parágrafo único. Poderão ser instituídos níveis diferenciados de credenciamento para as AC, de conformidade com a sua finalidade.

Art. 9º As AC devem prestar os seguintes serviços básicos:

I - emissão de certificados;
II - revogação de certificados;
III - renovação de certificados;

IV - publicação de certificados em diretório;
V - emissão de Lista de Certificados Revogados - LCR;
VI - publicação de LCR em diretório; e
VII - gerência de chaves criptográficas.

Parágrafo único. A disponibilização de certificados emitidos e de LCR atualizada será proporcionada mediante uso de diretório seguro e de fácil acesso.

Art. 10. Cabe às AR:

I - receber as requisições de certificação ou revogação de certificado por usuários, confirmar a identidade destes usuários e a validade de sua requisição e encaminhar esses documentos à AC responsável;

II - entregar os certificados assinados pela AC aos seus respectivos solicitantes.

CAPÍTULO III
DO MODELO OPERACIONAL

Art. 11. A emissão de certificados será precedida de processo de identificação do usuário, segundo critérios e métodos variados, conforme o tipo ou em função do maior ou menor grau de sua complexidade.

Art. 12. No processo de credenciamento das AC, deverão ser utilizados, além de critérios estabelecidos pela AGP e de padrões técnicos internacionalmente reconhecidos, aspectos adicionais relacionados a:

I - plano de contingência;
II - política e plano de segurança física, lógica e humana;
III - análise de riscos;
IV - capacidade financeira da proponente;
V - reputação e grau de confiabilidade da proponente e de seus gerentes;
VI - antecedentes e histórico no mercado; e
VII - níveis de proteção aos usuários dos seus certificados, em termos de cobertura jurídica e seguro contra danos.

Parágrafo único. O disposto nos incisos IV a VII não se aplica aos credenciamentos de AC Públicas.

Art. 13. Obedecidas às especificações da AGP, os órgãos e as entidades da Administração Pública Federal poderão implantar sua própria ICP ou ofertar serviços de ICP integrados à ICP-Gov.

Art. 14. A AC Privada, para prestar serviço à Administração Pública Federal, deve observar as mesmas diretrizes da AC Governamental, salvo outras exigências que vierem a ser fixadas pela AGP.

CAPÍTULO IV
DA POLÍTICA DE CERTIFICAÇÃO

Art. 15. Serão definidos tipos de certificados, no âmbito da ICP-Gov, que atendam às necessidades gerais da maioria das aplicações, de forma a viabilizar a interoperabilidade entre ambientes computacionais distintos, dentro da Administração Pública Federal.

§ 1º Serão criados certificados de assinatura digital e de sigilo, atribuindo-se-lhes os seguintes níveis de segurança, consoante o processo envolvido:

I - ultra-secretos;
II - secretos;
III - confidenciais;
IV - reservados; e
V - ostensivos.

§ 2º Os certificados, além de outros que a AGP poderá estabelecer, terão uso para:

I - assinatura digital de documentos eletrônicos;
II - assinatura de mensagem de correio eletrônico;
III - autenticação para acesso a sistemas eletrônicos; e
IV - troca de chaves para estabelecimento de sessão criptografada.

Art. 16. À AGP compete tomar as providências necessárias para que os documentos, dados e registros armazenados e transmitidos por meio eletrônico, óptico, magnético ou similar passem a ter a mesma validade, reconhecimento e autenticidade que se dá a seus equivalentes originais em papel.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

Art. 17. Para instituição da ICP-Gov, deverá ser efetuado levantamento das demandas existentes nos órgãos governamentais quanto aos serviços típicos derivados da tecnologia de Chaves Públicas, tais como, autenticação, sigilo, integridade de dados e irretratabilidade das transações eletrônicas.

Art. 18. O Glossário constante do Anexo II apresenta o significado dos termos e siglas em português, que são utilizados no sistema de Chaves Públicas.

Art. 19. Compete ao Comitê Gestor de Segurança da Informação a concepção, a especificação e a coordenação da implementação da ICP-Gov, conforme disposto no art. 4º, inciso XIV, do Decreto nº 3.505, de 13 de junho de 2000.

Art. 20. Fica estabelecido o prazo de cento e vinte dias, contados a partir da data de publicação deste Decreto, para especificação, divulgação e início da implementação da ICP-Gov.

Art. 21. Implementados os procedimentos para a certificação digital de que trata este Decreto, a Casa Civil da Presidência da República estabelecerá cronograma com vistas à substituição progressiva do recebimento de documentos físicos por meios eletrônicos.

Art. 22. Este Decreto entra em vigor na data de sua publicação.

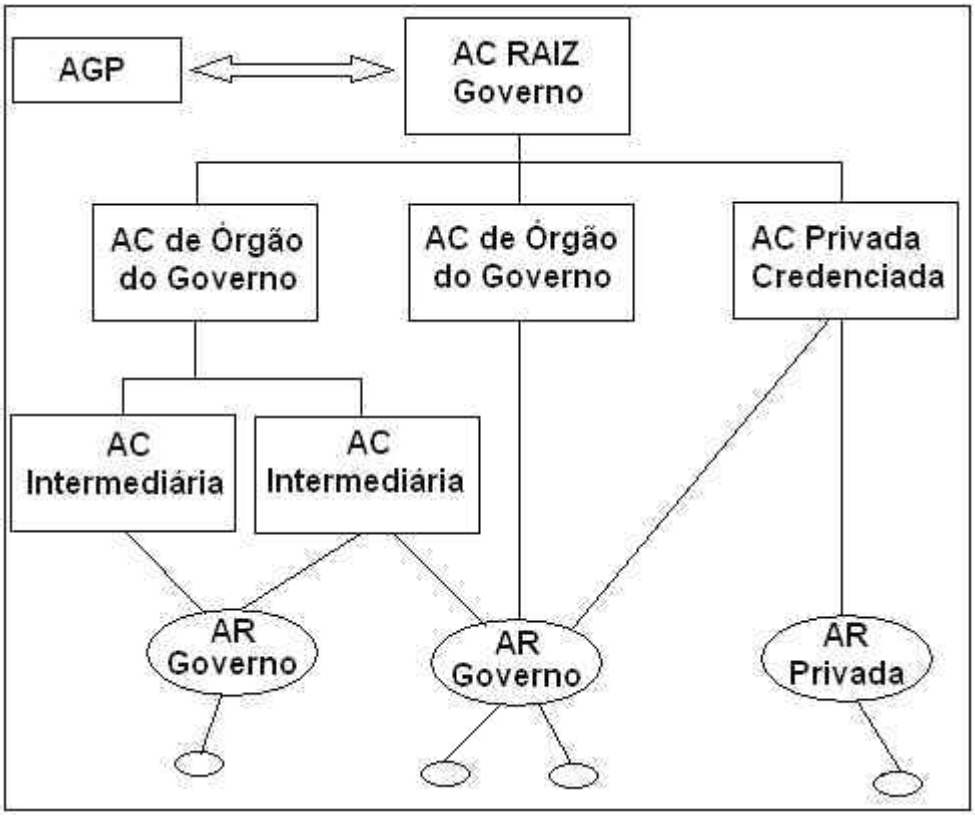
Brasília, 5 de setembro de 2000; 179º da Independência e 112º da República.

FERNANDO HENRIQUE CARDOSO
Guilherme Gomes Dias
Alberto Mendes Cardoso

Publicado no D.O.U. de 06.09.2000, Seção I, 1ª página.

ANEXO I

ARQUITETURA DA ICP-Gov



ANEXO II

GLOSSÁRIO

Autenticação *(Authentication)*	Processo utilizado para confirmar a identidade de uma pessoa ou
Autoridade Certificadora – AC	Entidade que emite certificados de acordo com as práticas definidas na
Autoridade Registradora – AR	Entidade de registro. Pode estar fisicamente localizada em uma AC ou
Assinatura Digital (*Digital Signature*)	Transformação matemática de uma mensagem por meio da utilização de

	desta com a chave privada da entidade assinante.
Autorização *(Authorization)*	Obtenção de direitos, incluindo a habilidade de acessar uma informação específica ou recurso de uma maneira específica.
Chave Privada *(Private Key)*	Chave de um par de chaves mantida secreta pelo seu dono e usada no sentido de criar assinaturas para cifrar e decifrar mensagens com as Chaves Públicas correspondentes.
Certificado de Chave Pública *(Certificate)*	Declaração assinada digitalmente por uma AC, contendo, no mínimo: ?? o nome distinto (DN – Distinguished Name) de uma AC, que emitiu o certificado; ?? o nome distinto de um assinante para quem o certificado foi emitido; ?? a Chave Pública do assinante; ?? o período de validade operacional do certificado; ?? o número de série do certificado, único dentro da AC; e ?? uma assinatura digital da AC que emitiu o certificado com todas as informações citadas acima.
Chave Pública *(Public Key)*	Chave de um par de chaves criptográficas que é divulgada pelo seu dono e usada para verificar a assinatura digital criada com a chave privada correspondente ou, dependendo do algoritmo criptográfico assimétrico utilizado, para cifrar e decifrar mensagens.
Cifração *(Encryption)*	Processo de transformação de um texto original ("plaintext") em uma forma incompreensível ("ciphertext") usando um algoritmo criptográfico e uma chave criptográfica.
Credenciamento *(Accreditation)*	Processo de aprovação de políticas e procedimentos de uma AC, de forma que a mesma seja autorizada a participar de uma ICP.
Criptografia *(Cryptography)*	Disciplina que trata dos princípios, meios e métodos para a transformação de dados, de forma a proteger a informação contra acesso não autorizado a seu conteúdo.
Criptografia de Chave Pública	Tipo de criptografia que usa um par de chaves criptográficas

(Public Key Cryptography)	matematicamente relacionadas. As Chaves Públicas podem ficar disponíveis para qualquer um que queira cifrar informações para o dono da chave privada ou para verificação de uma assinatura digital criada com a chave privada correspondente. A chave privada é mantida em segredo pelo seu dono e pode decifrar informações ou gerar assinaturas digitais.
Declaração de Regras Operacionais – DRO *(Certification Practice Statement – CPS)*	Documento que contém as práticas e atividades que uma AC implementa para emitir certificados. É a declaração da entidade certificadora a respeito dos detalhes do seu sistema de credenciamento e as práticas e políticas que fundamentam a emissão de certificados e outros serviços relacionados.
Emissão de Certificado *(Certificate Issuance)*	Emissão de um certificado por uma AC após a validação de seus dados, com a subseqüente notificação do requente sobre o conteúdo do certificado.
Gerenciamento de Certificado *(Certificate Management)*	Ações tomadas por uma AC, baseadas na sua DRO após a emissão do certificado, como armazenamento, disseminação e a subseqüente notificação, publicação e renovação do certificado. Uma AC considera certificados emitidos e aceitos como válidos a partir da sua publicação.
Infra-Estrutura de Chaves Públicas – ICP *(Public Key Infrastructure – PKI)*	Arquitetura, organização, técnicas, práticas e procedimentos que suportam, em conjunto, a implementação e a operação de um sistema de certificação baseado em criptografia de Chaves Públicas.
Integridade de Mensagem (Message Integrity)	Garantia de que a mensagem não foi alterada durante a sua transferência, do emissor da mensagem para o seu receptor.
Irretratabilidade *(Nonrepudiation)*	Garantia de que o emissor da mensagem não irá negar posteriormente a autoria de uma mensagem ou participação em uma transação, controlada pela existência da assinatura digital que somente ele pode gerar.
Lista de Certificados Revogados – *LCR (Certification Revogation List – CRL)*	Lista dos números seriais dos certificados revogados, que é digitalmente assinada e publicada em um repositório. A lista contém ainda a data da emissão do certificado revogado e outras informações, tais

	como as razões específicas para a sua revogação.
Mensagem *(Message)*	Registro contendo uma representação digital da informação, como um dado criado, enviado, recebido e guardado em forma eletrônica.
Par de Chaves *(Key Pair)*	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.
Política de Certificação – PC *(Certificate Police – CP)*	Documento que estabelece o nível de segurança de um determinado certificado
Raiz *(Root)*	Primeira AC em uma cadeia de certificação, cujo certificado é auto-assinado, podendo ser verificado por meio de mecanismos e procedimentos específicos, sem vínculos com este.
Registro *(Record)*	Informação registrada em um meio tangível (um documento) ou armazenada em um meio eletrônico ou qualquer outro meio perceptível.
Repositório *(Repository)*	Sistema confiável e acessível "on-line" para guardar e recuperar certificados e informações relacionadas com certificados.
Revogação de Certificado *(Certificate Revogation)*	Encerramento do período operacional de um certificado, podendo ser, sob determinadas circunstâncias, implementado antes do período operacional anteriormente definido.
Sigilo *(Confidentiality)*	Condição na qual dados sensíveis são mantidos secretos e divulgados apenas para as partes autorizadas.
Sistema Criptográfico Assimétrico *(Asymmetric Criptosystem)*	Sistema que gera e usa um par de chaves seguras, consistindo de uma chave privada para a criação de assinaturas digitais ou decodificar de mensagens criptografadas e uma Chave Pública para verificação de assinaturas digitais ou de mensagens codificadas.