

SUMÁRIO

1. **INTRODUÇÃO**

2. **AMBIENTE CONCEITUAL DA ICP-Brasil**
 - 2.1 Criptografia
 - 2.1.1 Criptografia Simétrica
 - 2.1.1.1 Criptografia Assimétrica
 - 2.2 Assinatura Digital com Criptografia de Chave Pública
 - 2.3 Certificado Digital, Autoridade Certificadora, Autoridade de Registro

3. **ICP-Brasil**
 - 3.1 Antecedentes
 - 3.2 Integrantes da ICP-Brasil – Funções
 - 3.2.1 Comitê Gestor
 - 3.2.2 Autoridade Certificadora Raiz
 - 3.2.3 Autoridade Certificadora
 - 3.2.4 Autoridade de Registro
 - 3.2.5 Outros Comentários sobre a organização da ICP-Brasil
 - 3.3 Documentos Básicos da ICP-Brasil
 - 3.3.1 Política de Segurança
 - 3.3.2 Declaração de Práticas de Certificação
 - 3.3.3 Critérios e Procedimentos de Credenciamento de Entidades da ICP-Brasil
 - 3.3.4 Requisitos Mínimos das Políticas de Certificado da ICP-Brasil
 - 3.3.5 Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil
 - 3.4 Informações Adicionais

4. **LEGISLAÇÃO**
 - 4.1 Lei
 - 4.2 Medida Provisória
 - 4.3 Decretos
 - 4.4 Resoluções

1. INTRODUÇÃO

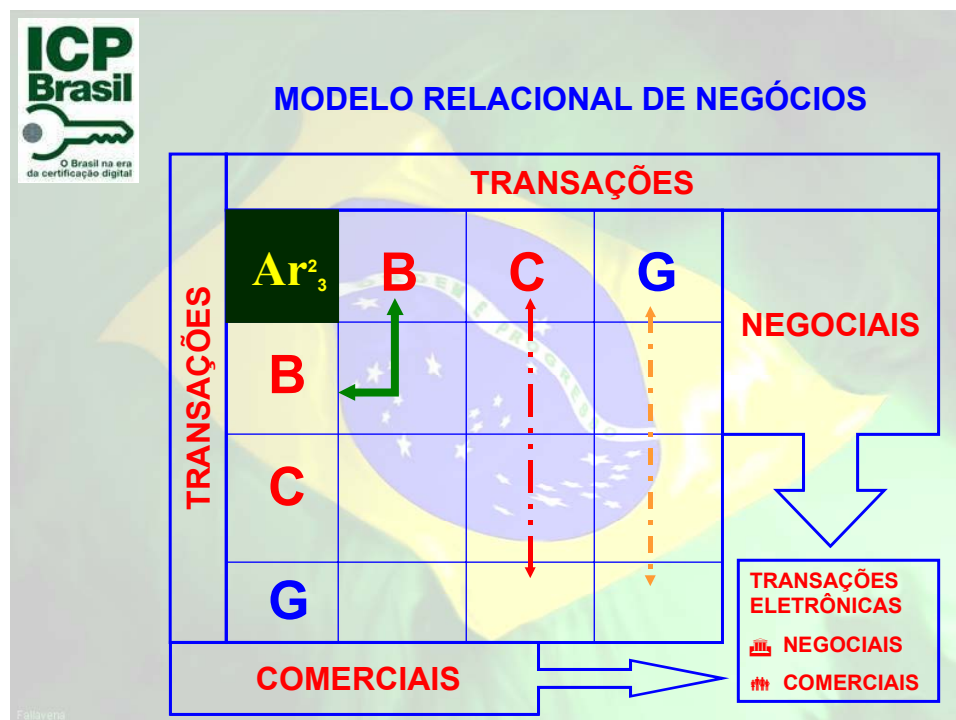
Desde muito, a informação tem se constituído em importante elemento nas relações entre os seres humanos. O desenvolvimento dos meios de comunicação, cuja sofisticação atingiu elevados níveis na sociedade atual, permitiu a implementação de comunicações em tempo real, por meio de redes de transporte de dados e da INTERNET.

Essa expansão do mundo digital leva à conclusão de estarmos vivendo uma revolução, em escala planetária, onde estamos colaborando, e também intervindo, na construção de uma nova sociedade, a chamada Sociedade da Informação.

O paradigma que emerge dessa revolução é a prevalência da informação eletrônica, gerando um conjunto de novas relações econômicas e sociais, vivenciadas pela sociedade de maneira cada vez mais natural.

Esse conjunto de transações eletrônicas, denominado negócios eletrônicos – “e-business”, ocorre entre vários atores:

- B - business – empresas
- C – cidadãos
- G – governo



Esse conjunto de atores pode se relacionar de forma matricial, implementando negócios eletrônicos de diversos tipos, entre eles o comércio eletrônico, a conhecida relação B2B.

A informação, dentro das transações eletrônicas, deve ter os seguintes requisitos:

- **Disponibilidade:** o documento, ou informação, deve estar disponível ininterruptamente, para novo tratamento ou utilização.
- **Integridade:** fidelidade do documento ao teor original, sem sofrer qualquer alteração.
- **Confidencialidade:** a informação relacionada a um indivíduo, empresa, ou entidade deve ser protegida da ação indevida de terceiros, seja para conhecer ou tratar essa informação;
- **Autenticidade:** há que ser garantida a autoria, origem e destino do documento eletrônico;
- **Irretratabilidade:** é a garantia de que uma transação depois de efetuada não pode ser negada.

A implementação de uma política de segurança da informação adequada irá atender a todos os requisitos de segurança, fazendo com que a informação detenha os atributos necessários a sua utilização de forma ampla e confiável.

As soluções tecnológicas para implementar essa política podem ser variadas. Uma das mais utilizadas atualmente, disseminada pelo uso de redes de computadores, é a criptografia. No entanto, a utilização de métodos criptográficos distintos, sem gerenciamento, nem padrões específicos, ao invés de agilizar os negócios eletrônicos, pode resultar na sua inviabilização.

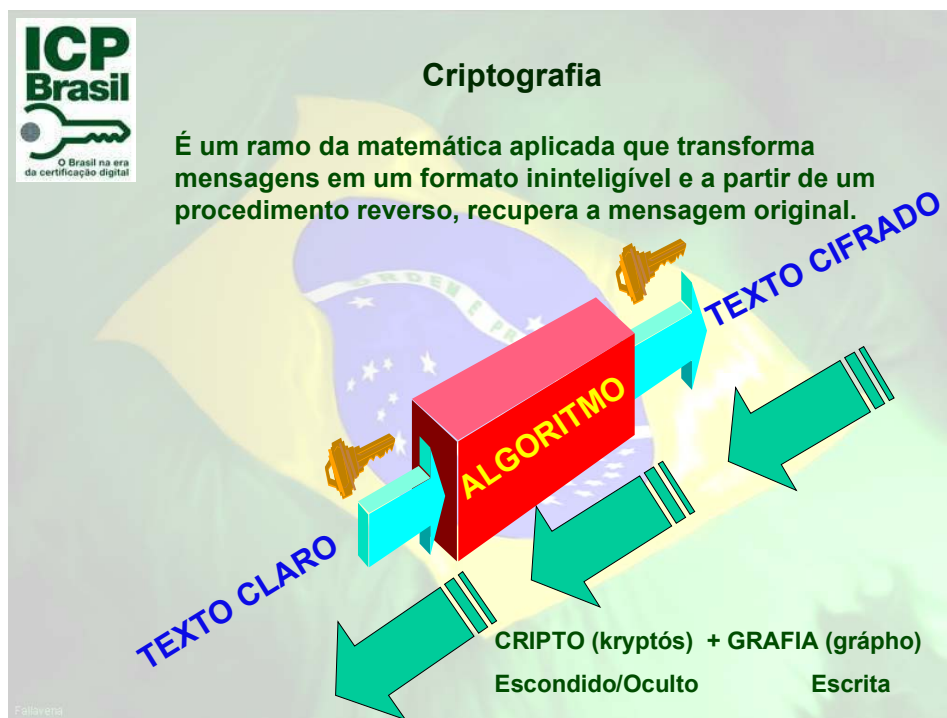
2. AMBIENTE CONCEITUAL DA ICP-Brasil

2.1 **Criptografia**

A criptografia se constitui em um conjunto de métodos e técnicas destinadas a proteger o conteúdo de uma informação, tanto em relação a modificações não autorizadas quanto a alteração de sua origem, sendo uma das técnicas que possibilitam o atendimento dos requisitos básicos de segurança da informação.

A informatização da criptografia tornou suas aplicações mais popularizadas e disseminadas, permitindo o desenvolvimento de aplicações cada vez mais sofisticadas.

A confidencialidade de um documento – texto claro – será garantida quando ele for processado por um conjunto de operações, sendo transformado em um texto cifrado. O emissor do documento envia, então, o texto cifrado, que será reprocessado pelo receptor, transformando-o, novamente, em texto claro, igual ao emitido.



O conjunto de regras que determina as transformações do texto claro é chamado de algoritmo (uma seqüência de operações) e o parâmetro que determina as condições da transformação é chamado de chave.

Para o usuário da criptografia, é fundamental ter a chave que iniciará o processo de cifração, ou seja, é necessário alimentar seu equipamento com a informação que iniciará o processo de criptografia do texto claro. Existem dois tipos de criptografia: simétrica e assimétrica

2.1.1 Criptografia Simétrica

A criptografia simétrica é baseada em algoritmos que dependem de uma mesma chave, denominada chave secreta, que é usada tanto no processo de cifrar quanto no de decifrar o texto cifrado. Somente o emissor e o receptor devem conhecer a chave secreta, a qual necessita de proteção em relação ao ambiente externo, para que usuários não autorizados não tenham acesso a informação. Isso significa dizer que a segurança da comunicação depende da garantia de segredo da chave secreta, que só deve ser de conhecimento do emissor e do receptor.

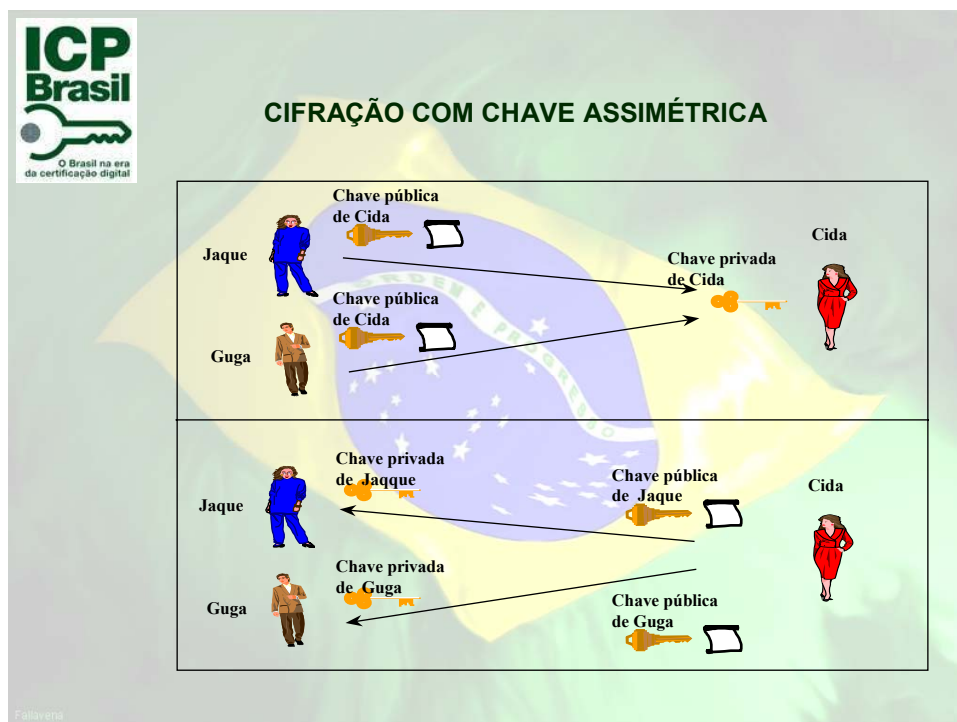


2.1.2 Criptografia Assimétrica

A criptografia assimétrica baseia-se em algoritmos que utilizam duas chaves diferentes, relacionadas matematicamente através de um algoritmo, de forma que o texto cifrado pela chave 1 do par somente poderá ser decifrado pela chave 2 do mesmo par.

As duas chaves envolvidas na criptografia assimétrica são denominadas chave pública e chave privada. A chave pública pode ser obtida pelo público em geral, enquanto que a chave privada somente deve ser de conhecimento de seu titular. Da mesma forma que no sistema de criptografia simétrica, a segurança da comunicação depende da garantia de segredo da chave privada, que só deve ser de conhecimento do de seu titular.

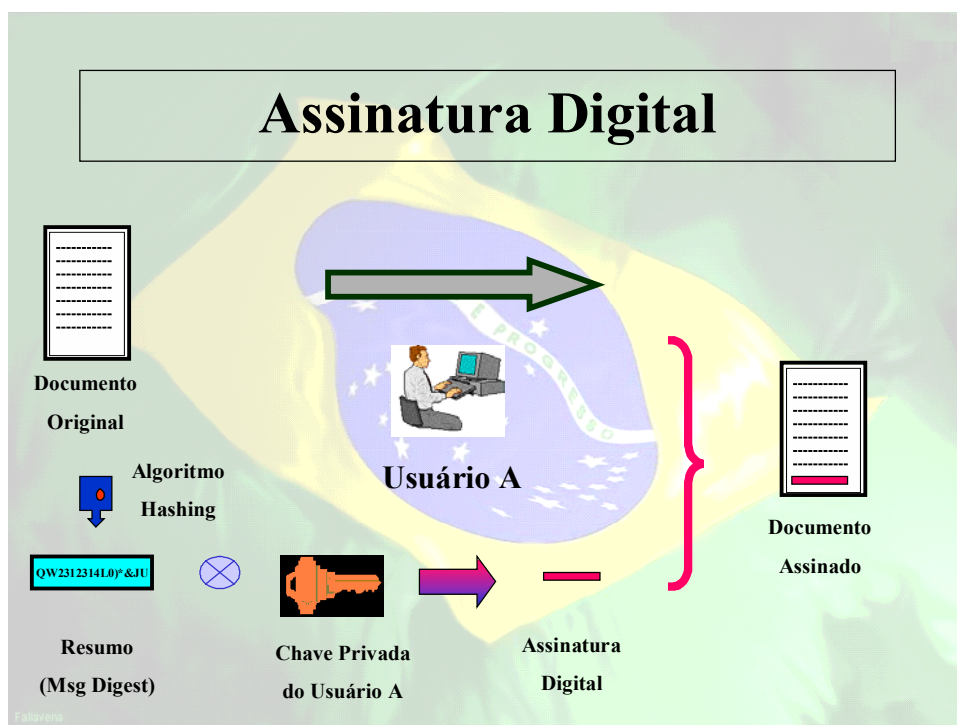
O emissor processa seu documento com a chave pública do receptor, que é conhecida. O texto cifrado somente poderá ser decifrado pelo receptor previsto, uma vez que somente ele tem a chave privada relacionada à chave pública que orientou a criptografia do documento emitido. Desta forma, fica atendido o requisito de confidencialidade da informação.



2.2 Assinatura Digital com Criptografia de Chave Pública

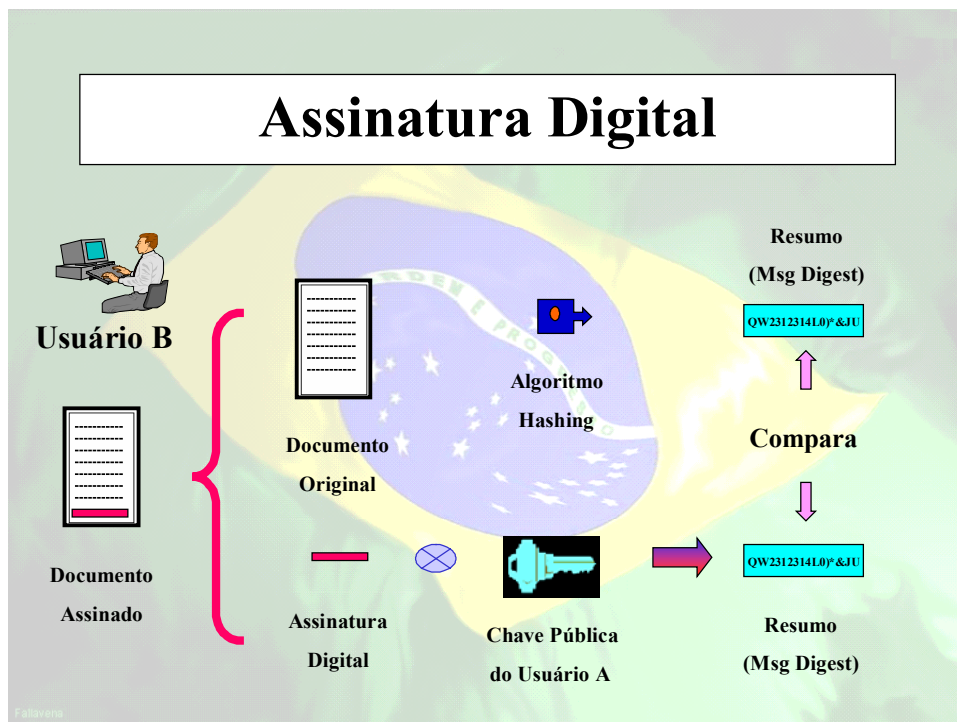
A cifração do documento eletrônico atende ao requisito de confidencialidade da informação transmitida. Para atender aos requisitos de integridade e autenticidade são implementadas outras ações, gerando um documento assinado digitalmente.

A primeira etapa do processo de geração de um documento assinado digitalmente é aplicar uma função de resumo (hash) ao documento eletrônico, obtendo-se uma seqüência de tamanho fixo, única para cada documento. Nota-se que, a partir do resumo, nome dado ao resultado da função hash, não é possível recuperar o documento original, ou seja, a função hash é unidirecional.



Na segunda etapa do processo, esse resumo será então cifrado com a chave privada do emissor do documento, gerando um arquivo eletrônico que representará a assinatura digital do emissor. Essa assinatura será anexada ao documento eletrônico original, compondo a mensagem ou arquivo, que será transmitido ao receptor. Uma assinatura digital está associada a cada documento emitido.

Na terceira etapa do processo, o receptor recebe a mensagem ou arquivo – o documento original mais a assinatura. Aplica a função de hash, ao documento original, obtendo um resultado, aqui chamado **resumo1**.



Em seguida, a assinatura é decifrada utilizando-se a chave pública do emissor, obtendo-se assim o resumo. Compara-se O **resumo** com o **resumo1**.

Caso os resumos sejam iguais, é possível concluir que:

- O documento está íntegro; e
- O documento foi realmente enviado pelo emissor porque a chave pública do receptor conseguiu decifrá-lo;

2.3 Certificado Digital, Autoridade Certificadora e Autoridade de Registro.

A associação de uma chave pública a um determinado usuário é feita através de um certificado digital. O padrão X.509 estabelece que um certificado digital deve conter, entre outras, as seguintes informações:

- Versão;
- Número de série;
- O período de validade;
- Emissor;
- Usuário;
- Chave pública do usuário; e

- A assinatura digital do emissor.

A veracidade dos dados contidos no certificado digital é assegurada pela entidade que o emite, a chamada Autoridade Certificadora. A aceitabilidade do certificado dependerá da confiança dos usuários nas práticas de trabalho da autoridade Certificadora.

A Autoridade de Registro tem o papel de verificar a identidade do usuário solicitante do certificado, de forma presencial e atendendo a padrões estabelecidos pela Autoridade Certificadora a qual está vinculada.

3. **Infra-Estrutura de Chaves Públicas do Brasil - ICP-Brasil**

3.1 **Antecedentes**

A decisão do Governo Brasileiro de implantar uma Infra-Estrutura de Chaves Públicas decorreu da necessidade de regulamentar a questão da certificação digital, considerando a disseminação do uso da tecnologia da informação na sociedade.

A estruturação da ICP-Brasil considerou os seguintes princípios básicos:


- **Responsabilidade:** a atribuição de responsabilidade aos proprietários, prestadores de serviço e usuários de sistemas de informação e outras partes envolvidas com a segurança dos sistemas de informação devia ser explicitada e documentada;
- **Conhecimento:** os proprietários, prestadores de serviço e usuários dos sistemas de informação deviam adquirir conhecimentos apropriados da existência e abrangência geral das medidas, práticas e procedimentos relacionados à segurança dos sistemas de informação, para fomentar a confiança nos sistemas de informação que iriam formar a ICP-Brasil;
- **Ética:** os sistemas de informação que iriam integrar a ICP-Brasil e os seus mecanismos de segurança deveriam ser fornecidos e utilizados de forma que os direitos e interesses legítimos de outrem fossem respeitados;
- **Multidisciplinaridade:** as normas, práticas e procedimentos relacionados com a segurança dos sistemas de informação integrantes da ICP-Brasil deveriam considerar pontos de vista relevantes, de natureza técnica, administrativa, organizacional, operacional, comercial, educacional e jurídica;
- **Proporcionalidade:** a ICP-Brasil deveria contemplar níveis de segurança, normas, práticas e procedimentos compatíveis com a importância, e o valor dos sistemas de informação que a utilizem, considerando-se os ambientes específicos envolvidos;
- **Integração:** as normas, práticas e procedimentos relacionados à segurança dos sistemas de informação deveriam ser coordenados e integrados de modo a criar um conjunto harmônico e coerente de segurança da informação, para o governo e sociedade civil;
- **Atualização:** a segurança dos sistemas de informação integrantes da ICP-Brasil deverá ser reavaliada periodicamente, na medida em que os sistemas de informação e as exigências ligadas à sua segurança variem em relação ao momento tecnológico considerado;
- **Escalabilidade:** ter a perspectiva de crescimento que abrange tanto o número de aplicações quanto a quantidade de usuários; e
- **Interoperabilidade:** preferencialmente, os sistemas deveriam obedecer ao paradigma de sistemas abertos, de modo a se reduzir ao máximo as incertezas relacionadas com a integração de outros sistemas à infraestrutura existente.

Foram desenvolvidos estudos para escolha da solução técnica de implantação da ICP-Brasil, os quais levaram em consideração as experiências desenvolvidas na normalização e padronização internacionais adotadas por diversos países, assim como o sistema político adotado no Brasil, as características sociais, culturais,

administrativas e técnicas observadas em outros projetos do Poder Executivo Federal.

Uma das principais características da ICP-Brasil é sua estrutura hierárquica. Nas estruturas hierárquicas que utilizam Autoridade Certificadora Raiz, o contrato de adesão é subordinado a um processo de credenciamento, no qual é avaliada e validada a conformidade das políticas e práticas de cada ambiente.

Como esse era um dos objetivos desejados pelo Poder Executivo Federal, a adoção dessa solução hierárquica foi adequada às necessidades identificadas, onde o estabelecimento de relações de confiança entre as Autoridades Certificadoras componentes proporcionaria significativa economia de escala e recursos técnicos. A solução proporciona um trâmite da informação sem as etapas intermediárias de certificação, já que tais etapas não agregam valor ao conteúdo e apenas estabelecem uma burocracia eletrônica. Estas características proporcionam total conformidade de todas as Autoridades Certificadoras, sejam elas públicas ou privadas, que integram uma infra-estrutura de chaves públicas.



INFRA-ESTRUTURA DE CHAVES PÚBLICAS – ICP-Brasil

NORMATIVO	POLÍTICAS, DIRETRIZES, NORMAS, REGRAS OPERACIONAIS
CG-ICP-Brasil	Características (regulador de atividades econômico produtivas) formulador de políticas com poder de normatização (órgão sistêmico),
CRENCIAMENTO	CREDITAÇÃO, AUDITAGEM E CERTIFICAÇÃO
AC Raiz	Características órgão creditor, auditor e fiscalizador das políticas diretrizes, normas e regras (regulamentos técnicos) definidos pelo CG-ICP, além de fiscalização (auditoria) e poder de polícia (fazenda pública).
OPERACIONAL	BASE OPERACIONAL DA ICP- Brasil
AC Pub Pri	EXPEDIÇÃO DE CERTIFICADOS DE CHAVES PÚBLICAS E DE SIGILO DIGITAIS
AR Pub Pri	IDENTIFICAÇÃO, CADASTRAMENTO, LANÇAMENTO

Como requisito fundamental para a implantação da ICP-Brasil, considerou-se imprescindível a formação de uma base material formada por um conjunto de hardware, software, políticas e procedimentos, que daria a forma de sua arquitetura.

3.2 Os integrantes da ICP-Brasil – Funções

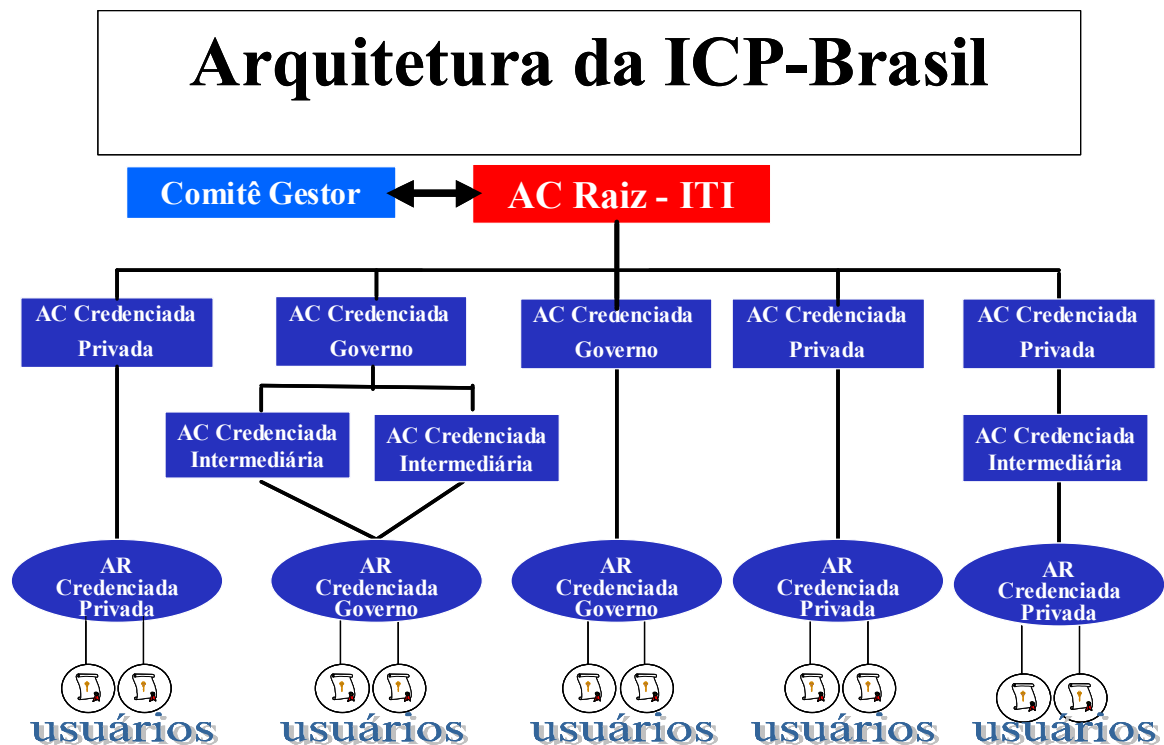
A estrutura hierárquica da ICP-Brasil é determinada pela MP 2200-2, de 24 de agosto de 2001, que instituiu a ICP-Brasil e estabeleceu as competências de cada tipo de entidade na estrutura.

As determinações do citado diploma legal estão em consonância com normas internacionais, como, por exemplo, a ISO, Guias 60 e 61. Assim, obtém-se aceitabilidade internacional para a ICP-Brasil, facilitando, ainda, a interoperabilidade com os sistemas de certificação digital dos demais países.

São previstos três níveis nessa arquitetura: o nível de gestão, o nível de credenciamento e o nível de operação, com entidades e funções específicas previstas para cada uma delas.

O nível de gestão contempla a gestão geral e a normalização da ICP-Brasil. O nível de credenciamento contempla a conformidade dos métodos e processos a serem utilizados pelas instituições operacionais do sistema, com base nos regulamentos e normas preestabelecidos. Finalmente, o nível de operação executa atividades de registro, certificação e guarda de documentos do usuário final, para emissão do respectivo certificado digital.

A atuação de cada uma dessas entidades é embasada por regulamentos, normas e padrões específicos, necessários e suficientes para a integração das instituições, apresentando condições adequadas de confiabilidade técnica de gestão e operação.



3.2.1 **Comitê Gestor**

As funções do Comitê Gestor, criado pela MP 2200-2, e regulamentado pelo Decreto nº 3.872, de 10 de julho de 2001, podem ser resumidamente descritas:

- Estabelecer, avaliar e aprovar políticas, critérios e normas no âmbito da ICP-Brasil seja para as Autoridades Certificadoras e Registradoras ou para supervisão da Autoridade Certificadora Raiz;
- Fomentar e implementar acordos internacionais relativos a certificação cruzada, regras de interoperabilidade e certificação bilateral, entre outros.

3.2.2 **Autoridade Certificadora Raiz**

A Autoridade Certificadora Raiz da cadeia da ICP-Brasil é responsável pelo credenciamento na cadeia hierárquica, operando a partir de definições da Autoridade Gestora de Políticas – o Comitê Gestor.

Em termos legais, a Medida Provisória 2200-2 estabelece, como função básica da AC Raiz, a execução das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor, tendo como competências:

- Emitir, expedir, distribuir, revogar e gerenciar certificados de Autoridades do nível imediatamente inferior ao seu;
- Gerenciar a lista de certificados emitidos, revogados e vencidos; e
- Executar fiscalização e auditoria da ACs, ARs e prestadores de serviço habilitados na ICP-Brasil.

De acordo com a determinação da Medida Provisória 2.200, o ITI – Instituto Nacional de Tecnologia da Informação é a AC Raiz da ICP-Brasil. O ITI está estruturado como autarquia federal, vinculada à Casa Civil da Presidência da República.

3.2.3 **Autoridade Certificadora**

Uma Autoridade Certificadora é a primeira entidade do nível operacional do sistema. Sua primeira responsabilidade é emitir certificados digitais vinculando uma chave pública ao seu titular, após receber credenciamento pela AC Raiz. Suas competências, de acordo com o previsto na MP 2200-2, são:

- Emitir, expedir, distribuir, revogar e gerenciar os certificados;
- Divulgar aos usuários as listas de certificados revogados; e
- Manter registros de suas operações.

Observa-se que, além de atender aos requisitos técnicos, a AC tem a obrigação da transparência em suas atividades, seja para garantir segurança, na medida

em que o usuário tem conhecimento dos certificados revogados, seja para consulta a operações já realizadas.

Poderão se credenciar como Autoridades Certificadoras tanto entidades privadas e órgãos públicos, desde que cumpram os requisitos mínimos estabelecidos pela AC Raiz.

3.2.4 **Autoridade de Registro**

Uma Autoridade Registro é a interface do sistema ICP-Brasil com o usuário final. Ela é vinculada à determinada Autoridade Certificadora e tem como competências:

- Identificar e cadastrar usuários, de forma presencial;
- Encaminhar solicitações de certificados à respectiva AC;
- Manter registros de suas operações.

Da mesma forma, podem ser credenciadas como AR tanto entidades privadas como órgãos públicos.

3.2.5 **Outros comentários sobre a organização da ICP-Brasil**

A estrutura hierárquica do sistema ICP-Brasil implica a permissão para a AC Raiz, ou outra AC, certificar apenas o nível hierárquico imediatamente inferior ao seu. Exceção é feita aos acordos de certificação lateral ou cruzada, quando aprovados pelo Comitê Gestor.

É importante ressaltar que a regulamentação estabelecida pela MP 2200-2 não impede que sejam emitidos e utilizados certificados digitais em transações por entidades não credenciadas a ICP-Brasil. O diferencial de qualidade, que pode fazer uma entidade se credenciar de acordo com as regras estabelecidas, é a presunção de validade jurídica da transação efetuada.

3.3 **Os Documentos Básicos da ICP-Brasil**

3.3.1 **Política de Segurança**

A Política de Segurança – PS, da ICP-Brasil, aprovada pela Resolução nº 2, de 25 de setembro de 2001, do Comitê Gestor, é documento que estabelece as diretrizes de segurança para todos os integrantes do sistema, devendo ser referência para as entidades elaborarem suas normas e procedimentos de segurança.

As regras gerais da PS estabelecem o princípio de gestão da segurança, abrangendo todos os recursos humanos, administrativos e tecnológicos das instituições ligadas à ICP-Brasil, determinando a ampla divulgação de todos os procedimentos previstos para garantir a segurança adequada.

3.3.2 **Declaração de Práticas de Certificação da AC Raiz**

A Declaração de Práticas de Certificação – DPC, da AC Raiz, foi aprovada pela Resolução nº 1, de 25 de setembro de 2001, do Comitê Gestor da ICP-Brasil.

Este documento descreve as práticas e procedimentos empregados pela Autoridade Certificadora Raiz da Infra-estrutura de Chaves Públicas Brasileira na execução dos seus serviços.

A AC Raiz possui o certificado de nível mais alto na ICP-Brasil. Este certificado contém a chave pública correspondente à chave privada da AC Raiz, utilizada para assinar seu próprio certificado, os certificados das AC de nível imediatamente subsequente ao seu e sua LCR (Lista de Certificados Revogados).

A estrutura dessa DPC está baseada na RFC 2527 (Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework).

3.3.3 Critérios e Procedimentos de Credenciamento de entidades integrantes da ICP-Brasil

A Resolução nº 6, de 22 de novembro de 2001, do Comitê Gestor, aprovou os Critérios e Procedimentos para Credenciamento de Entidades integrantes da ICP-Brasil. Esse documento, portanto, apresenta critérios para credenciamento, manutenção do credenciamento e descredenciamento de Autoridades Certificadoras – ACs e Autoridades Registradoras – AR, na ICP-Brasil.

Para a ação de credenciamento, deve ser atendido um conjunto de requisitos comuns às ACs e ARs, no que tange à personalidade jurídica, de qualificação econômico-financeira e de atendimento aos requisitos técnicos determinados pela ICP-Brasil. Adicionalmente, as ACs devem apresentar pelo menos uma candidata à AR, a relação de candidatos a prestadores de serviço de suporte, contratar seguro de responsabilidade civil para os serviços de certificação digital e de registro e, principalmente, ter todas as suas instalações em território nacional.

Em relação às ARs, os requisitos específicos para credenciamento relacionam-se à vinculação à determinada AC, à apresentação de candidatos a prestadores de serviços de suporte e a ter instalações no território nacional. Exceções a essa última regra podem ser admitidas, desde que aprovadas pelo Comitê Gestor.

3.3.4 **Requisitos Mínimos das Políticas de Certificado na ICP-Brasil**

A Resolução nº 7, de 12 de dezembro de 2001, do Comitê Gestor da ICP-Brasil aprovou o documento "Requisitos Mínimos para Políticas de Certificado na ICP-Brasil".

Esse documento prevê, inicialmente, 8 (oito) tipos de certificados, cuja numeração é crescente de acordo com o aumento dos níveis de segurança previstos. Os tipos são:

- Certificados de Assinatura Digital: A1, A2, A3 e A4
- Certificados de Sigilo: S1, S2, S3 e S4

Os certificados de assinatura digital serão utilizados em aplicações como confirmação de identidade web, correio eletrônico, transações on-line, redes privadas virtuais, cifração de chaves de sessão e assinatura de documentos eletrônicos com verificação de integridade de suas informações. Os Certificados de Sigilo serão usados em aplicações como cifração de documentos, bases de dados e outras informações eletrônicas.

Seqüencialmente, o documento estabelece os itens que devem estar contidos nas Políticas de Certificados – PC, das Autoridades Certificadoras integrantes da ICP-Brasil. Esses itens se referem às obrigações e direitos das partes envolvidas, às respectivas responsabilidades, inclusive financeiras, às tarifas a serem cobradas pela AC, à disponibilidade das informações e repositório, à auditoria de conformidade e à classificação de sigilo das informações.

Posteriormente, é definido como uma Autoridade de Registro – AR, identificará e autenticará o solicitante do certificado, seja ele pessoa física ou jurídica. Salienta-se que, mesmo no caso de pessoa jurídica, o certificado será emitido em nome de um responsável da instituição. Além disso, a PC de determinada Autoridade Certificadora também deverá estabelecer requisitos e procedimentos para solicitação, emissão, aceitação, suspensão e revogação de certificados, bem como da LCR – Lista de Certificados Revogados da respectiva AC.

A tabela a seguir, apresenta uma comparação entre os requisitos mínimos para cada tipo de certificado.

Tipo de Certificado	Chave Criptográfica			Validade Máxima do Certificado (anos)	Frequência de emissão da LCR (horas)	Tempo Limite de Revogação (horas)
	Tamanho (bits)	Processo de Geração	Mídia Armazenadora			
A1 e S1	1024	<i>software</i>	Repositório protegido por senha	1	48	72
A2 e S2	1024	<i>hardware</i>	Cartão Inteligente ou token, ambos sem capacidade de geração de chave e protegidos por senha	2	36	54
A3 e S3	1024	<i>hardware</i>	Cartão Inteligente ou token, ambos com capacidade de geração de chave e protegidos por senha, ou hardware criptográfico aprovado pelo CG da ICP-Brasil	3	24	36
A4 e S4	2048	<i>hardware</i>	Cartão Inteligente ou token, ambos com capacidade de geração de chave e protegidos por senha, ou hardware criptográfico aprovado pelo CG da ICP-Brasil	3	12	18

3.3.5 Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil

A Resolução nº 8, de 12 de dezembro de 2001, do Comitê Gestor da ICP-Brasil, aprovou o documento "Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil".

Esse documento estabelece os requisitos mínimos obrigatórios a serem atendidos pelas Autoridades Certificadoras – ACs, na elaboração das respectivas DPCs – Declaração de Práticas de Certificação. Uma DPC é o documento que descreve as práticas e procedimentos empregados pela AC na execução dos seus serviços.

Preliminarmente, é referido um conjunto de informações que irão caracterizar a AC e sua rede de AR, bem como determinar os titulares de certificados da AC.

Esse documento determina ainda as obrigações, direitos e responsabilidades, em padrões mínimos, que devem constar da DPC da AC, abrangendo a rede de ARs a ela vinculadas, a terceira parte (relying party) e os titulares de certificados.

3.4 **Informações Adicionais**

O ITI – Instituto Nacional de Tecnologia da Informação, Autoridade Certificadora Raiz, credenciou, até 12 de junho de 2002, as seguintes Autoridades Certificadoras:

- AC/PR – Autoridade Certificadora da Presidência da República;
- AC/SERPRO – Serviço Federal de processamento de Dados; e
- AC/SERASA – Centralização dos Serviços dos Bancos S/A

Estão em processo de credenciamento as seguintes entidades:

- AC CERTISIGN; e
- AC UNICERT

4. **LEGISLAÇÃO**

4.1 **LEI**

Lei nº9.983, de 14 de julho de 2000.

Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providências.

4.2 **MEDIDA PROVISÓRIA**

Medida Provisória nº2.200-2, de 24 de agosto de 2001.

Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências.

4.3 **DECRETOS**

Decreto nº3.505, de 13 de junho de 2000.

Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências.

Decreto nº3.872, de 18 de julho de 2001.

Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CGICP-Brasil, sua Secretaria-Executiva, sua Comissão Técnica Executiva e dá outras providências.

Decreto nº3.996, de 31 de outubro de 2001.

Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.

4.4 **RESOLUÇÕES**

Resolução nº1, de 25 de Setembro de 2001.

Aprova a Declaração de Práticas de Certificação da AC Raiz da ICP-Brasil.
"Este texto não substitui o publicado no D.O.U. de 26 de Setembro de 2001."

Resolução nº2, de 25 de Setembro de 2001.

Aprova a Política de Segurança da ICP-Brasil.
"Este texto não substitui o publicado no D.O.U. de 26 de Setembro de 2001."

Resolução nº3, de 25 de Setembro de 2001.

Resolve designar a seguinte Comissão para auditar a Autoridade Certificadora Raiz - AC Raiz e seus prestadores de serviços.
"Este texto não substitui o publicado no D.O.U. de 26 de Setembro de 2001."

Resolução nº4, de 22 de Novembro de 2001.

Altera a Declaração de Práticas de Certificação da AC Raiz da ICP-Brasil.
"Este texto não substitui o publicado no D.O.U. de 23 de Novembro de 2001."

Resolução nº5, de 22 de Novembro de 2001.

Aprova o Relatório de auditoria da AC Raiz.

"Este texto não substitui o publicado no D.O.U. de 23 de Novembro de 2001."

Resolução nº6, de 22 de Novembro de 2001.

Aprova os critérios e procedimentos de credenciamento das entidades integrantes da ICP-Brasil.

"Este texto não substitui o publicado no D.O.U. de 23 de Novembro de 2001."

Resolução nº7, de 12 de Dezembro de 2001.

Aprova os requisitos mínimos para políticas de certificado na ICP-Brasil.

"Este texto não substitui o publicado no D.O.U. de 23 de Dezembro de 2001."

Resolução nº8, de 12 de Dezembro de 2001.

Aprova os requisitos mínimos para as declarações de práticas de certificação das autoridades certificadoras da ICP-Brasil.

"Este texto não substitui o publicado no D.O.U. de 13 de Dezembro de 2001."

Resolução nº9, de 12 de Dezembro de 2001.

Estabelece regras transitórias para a ICP-Brasil.

"Este texto não substitui o publicado no D.O.U. de 13 de Dezembro de 2001."

Resolução nº10, de 14 de Fevereiro de 2002.

Estabelece as diretrizes da política tarifária da Autoridade Certificadora Raiz - AC Raiz da ICP-Brasil.

"Este texto não substitui o publicado no D.O.U. de 15 de Fevereiro de 2002."

Resolução nº11, de 14 de Fevereiro de 2002.

Altera os requisitos mínimos para as políticas de certificado na ICP-Brasil, a declaração de práticas de certificação da AC Raiz da ICP-Brasil, delega atribuições para a AC Raiz e dá outras providências.

"Este texto não substitui o publicado no D.O.U. de 15 de Fevereiro de 2002."

Resolução nº12, de 14 de Fevereiro de 2002.

Estabelece regras processuais para credenciamento na ICP-Brasil.

"Este texto não substitui o publicado no D.O.U. de 15 de Fevereiro de 2002."

Resolução nº13, de 26 de Abril de 2002.

Altera a declaração de práticas de certificação da AC Raiz da ICP-Brasil, os critérios e procedimentos de credenciamento das entidades integrantes da ICP-Brasil, os requisitos mínimos para as declarações de práticas de certificação das autoridades certificadoras da ICP-Brasil, os requisitos mínimos para as políticas de certificado na ICP-Brasil, e dá outras providências.

"Este texto não substitui o publicado no D.O.U. de 29 Abril de 2002."

Resolução nº14, de 10 de Junho de 2002.

Altera os critérios e procedimentos para credenciamento das entidades integrantes da ICP-Brasil e a Resolução nº12, de 14 de fevereiro de 2002, que estabelece regras processuais para credenciamento na ICP-Brasil.

"Este texto não substitui o publicado no D.O.U. de 11 de junho de 2002."

Resolução nº15, de 10 de Junho de 2002.

Estabelece as diretrizes para sincronização de frequência e de tempo na Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil.

"Este texto não substitui o publicado no D.O.U. de 11 de junho de 2002."

Resolução nº16, de 10 de Junho de 2002.

Estabelece as diretrizes para sincronização de frequência e de tempo na Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil.

"Este texto não substitui o publicado no D.O.U. de 11 de junho de 2002."