



**Infraestrutura de Chaves Públicas Brasileira**

**PROCEDIMENTOS PARA GERENCIAMENTO DA CHAVE  
SIMÉTRICA PARA GERAÇÃO DO IDN**

**DOC-ICP-05.04**

**Versão 2.1**

**06 de julho de 2017**



# Infraestrutura de Chaves Públicas Brasileira

## Sumário

CONTROLE DE ALTERAÇÕES.....	3
LISTA DE SIGLAS e ACRÔNIMOS.....	4
1. GERAÇÃO, ARMAZENAMENTO E DISTRIBUIÇÃO DA CHAVE.....	5
1.1 Geração e Armazenamento da Chave.....	5
1.2 Distribuição da Chave.....	5
1.2.1 Recebimento de Certificado Digital da Entidade.....	5
1.2.2 Exportação da Chave Criptográfica Simétrica.....	5
1.2.3 Importação da Chave Criptográfica Simétrica pela Entidade.....	5
1.2.4 Prazo para Distribuição da Chave Criptográfica Simétrica.....	5
2. PROTEÇÃO DA CHAVE.....	6
3. PRAZO DE VALIDADE.....	6
4. SUBSTITUIÇÃO DA CHAVE SIMÉTRICA.....	6
5. CÓPIA DE SEGURANÇA DE CHAVE.....	6
6. DOCUMENTOS REFERENCIADOS.....	7

## CONTROLE DE ALTERAÇÕES

<b>Resolução ou IN que aprovou alteração</b>	<b>Item Alterado</b>	<b>Descrição da Alteração</b>
<b>Resolução 123, de 06.07.2017 (Versão 2.1)</b>	1.2.3	Inclui a opção de certificação INMETRO para a importação da cópia da chave criptográfica simétrica gerada.
<b>Instrução Normativa nº 13, de 21.11.2016 (Versão 2.0)</b>	1, 3, 4 e 5.	Aprova a versão 2.0 - atualiza os procedimentos de geração, armazenamento, distribuição, proteção, validade e substituição de chaves utilizadas no IDN.
<b>Instrução Normativa nº 08, de 10.12.2015 (Versão 1.0)</b>		Aprova a versão 1.0 do Documento Procedimentos para Gerenciamento da Chave Simétrica para geração do IDN.

## LISTA DE SIGLAS e ACRÔNIMOS

<b>SIGLA</b>	<b>DESCRIÇÃO</b>
AC	Autoridade Certificadora
AC RAIZ	Autoridade Certificadora Raiz da ICP-BRASIL
DOC-ICP	Documentos Principais da ICP-BRASIL
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
IDN	Identificador de Registro Biométrico
ITI	Instituto Nacional de Tecnologia da Informação
PSBio	Prestador de Serviço Biométrico

## **1. GERAÇÃO, ARMAZENAMENTO E DISTRIBUIÇÃO DA CHAVE**

### **1.1 Geração e Armazenamento da Chave**

As chaves criptográficas simétricas serão geradas e armazenadas pela AC Raiz, em hardware seguro com atributos específicos que permitam o gerenciamento do seu ciclo de vida.

O algoritmo e o tamanho das chaves criptográficas simétricas geradas pela AC Raiz e utilizadas para geração do IDN pelas ACs estão definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

### **1.2 Distribuição da Chave**

#### **1.2.1 Recebimento de Certificado Digital da Entidade**

As entidades interessadas, devidamente credenciadas no âmbito da ICP-Brasil, deverão gerar certificado digital, sendo a chave privada correspondente gerada e armazenada em MSC próprio da entidade.

Este certificado deverá ser enviado ao ITI por correio eletrônico, assinado digitalmente pelo representante legal da entidade.

#### **1.2.2 Exportação da Chave Criptográfica Simétrica**

Após o recebimento do certificado digital encaminhado pela entidade, o ITI agendará cerimônia interna de extração da correspondente chave pública, que servirá para cifragem e exportação da chave criptográfica simétrica.

#### **1.2.3 Importação da Chave Criptográfica Simétrica pela Entidade**

A cópia da chave criptográfica simétrica gerada será importada em MSC homologado ou com certificação INMETRO, pertencente à entidade, seguindo formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

A importação da chave criptográfica simétrica será feita na presença de um representante legalmente constituído da entidade, acompanhado por representante da AC Raiz, em cerimônia específica, com data e hora previamente estabelecidas

Para fins de auditoria, essa cerimônia deverá produzir evidências que a chave criptográfica importada não poderá ser exportada. Caberá ainda ao representante legal da entidade assinar termo específico de importação de chave criptográfica produzida na AC Raiz da ICP-Brasil.

#### **1.2.4 Prazo para Distribuição da Chave Criptográfica Simétrica**

O ITI deverá providenciar a distribuição da chave criptográfica simétrica em no máximo 30(trinta) dias úteis, contados a partir do recebimento do certificado digital da entidade.

## **2. PROTEÇÃO DA CHAVE**

As chaves criptográficas simétricas da AC Raiz, ao serem exportadas, serão cifradas com a chave pública da entidade, que deverá manter a chave privada equivalente em MSC, para abrir o envelope digital seguindo as regras do esquema de cifragem.

Compete à AC Raiz acompanhar a evolução tecnológica para, quando necessário, atualizar os padrões e algoritmos criptográficos utilizados na ICP-Brasil, com a atualização do documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1].

## **3. PRAZO DE VALIDADE**

Toda chave simétrica gerada pela AC Raiz terá validade de 2 (dois) anos, podendo ser prorrogada por meio de ato normativo do ITI.

Para geração e distribuição de nova chave criptográfica simétrica deverão ser observadas as regras e procedimentos estabelecidos no item 1 deste documento.

## **4. SUBSTITUIÇÃO DA CHAVE SIMÉTRICA**

A AC Raiz pode, a qualquer momento, gerar uma nova chave criptográfica simétrica para geração dos IDNs da ICP-Brasil, observando as regras e procedimentos do item 1 do presente.

Assim que as entidades receberem da AC Raiz uma nova chave criptográfica simétrica, os indexadores IDN usados por entidades e PSBios deverão ser recalculados. Caso necessário, poderão ser mantidos os IDN antigos até a completa reindexação de todas as bases de dados.

O procedimento de substituição da chave criptográfica simétrica, incluindo a reindexação das bases de dados com IDNs recalculados, deve ser executado num prazo máximo de 15 (quinze) dias úteis, contados a partir da importação da chave simétrica pelas entidades, de maneira sincronizada entre entidades e PSBios, de forma a não causar indisponibilidades no sistema. No caso de comprometimento da chave criptográfica simétrica, esses procedimentos devem ocorrer em no máximo 2 (dois) dias úteis.

Após a reindexação das bases de dados, os PSBios deverão excluir permanentemente qualquer informação indexada pelo IDN gerado a partir da chave criptográfica simétrica anterior, devendo as entidades manter em seus registros a associação entre IDN antigo e o novo.

## **5. CÓPIA DE SEGURANÇA DE CHAVE**

Cabe à AC Raiz realizar cópias de segurança de todas as chaves criptográficas simétricas geradas, de forma a garantir a sua preservação, bem como a contingência do sistema de geração e distribuição das chaves.

## 6. DOCUMENTOS REFERENCIADOS

<b>Ref.</b>	<b>Nome do Documento</b>	<b>Código</b>
[1]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL.	DOC-ICP-01.01