Infraestrutura de Chaves Públicas Brasileira

PROCEDIMENTOS PARA GERENCIAMENTO DA CHAVE SIMÉTRICA PARA GERAÇÃO DO IDN

DOC-ICP-05.04

versão 1.0

30 de setembro de 2015

Sumário

CONTROLE DE ALTERAÇÕES

Resolução ou IN que aprovou alteração	Item Alterado	Descrição da Alteração
Instrução Normativa nº 08, de 10.12.2015 (versão 1.0)		Aprova a versão 1.0 do Documento Procedimentos para Gerenciamento da Chave Simétrica para geração do IDN.

LISTA DE SIGLAS e ACRÔNIMOS

SIGLA	DESCRIÇÃO
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 E DISTRIBUIÇÃO DA CHAVE

1.1 Geração da chave

As chaves criptográficas simétricas serão geradas pela própria AC Raiz, em hardware seguro e através de sistema específico que permita o gerenciamento do ciclo de vida das chaves, bem como a sua custódia por no mínimo 3 (três) detentores.
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 Entrega da chave privada à entidade

A cópia da chave criptográfica simétrica será entregue às ACs credenciadas no âmbito da ICP-Brasil mediante solicitação e consequente autorização, para armazenamento no hardware específico e homologado da AC, em formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL[1]. Para ACs em credenciamento, a entrega da cópia da chave estará condicionada ao deferimento do seu credenciamento.
A entrega da chave criptográfica simétrica será feita ao representante legalmente constituído da AC, em cerimônia específica, em data e hora previamente estabelecidas pela AC Raiz. Todos os eventos ocorridos nessa cerimônia são registrados para fins de auditoria.
Sempre que houver a entrega de uma chave criptográfica simétrica, um representante da AC Raiz acompanhará o processo de importação no hardware da AC.

2. PROTEÇÃO DA CHAVE

As chaves criptográficas simétricas da AC Raiz serão exportadas cifradas com a chave pública da AC, que deve possuir a chave privada equivalente para abrir o envelope digital seguindo as regras do esquema de cifragem.
Compete à AC Raiz acompanhar a evolução tecnológica e, 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

A chave simétrica gerada pela AC Raiz terá validade de 2 (dois) anos, podendo ser prorrogada por meio de ato normativo do ITI. A nova chave criptográfica simétrica será entregue ao representante legalmente constituído das ACs, em cerimônia específica, conforme estabelecido no item 1.2 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, que será entregue ao representante legalmente constituído da AC, em cerimônia específica, após convocação pela AC Raiz.

Assim que as ACs receberem da AC Raiz a chave criptográfica simétrica substituída, as ACs e PSBios deverão ter seus indexadores IDN recalculados podendo, temporariamente, utilizar o IDN antigo juntamente com o IDN novo até a completa reindexação de todas as bases de dados dos PSBios.
O procedimento de substituição da chave criptográfica simétrica, incluindo a indexação dos IDNs recalculados, deve ser executado num prazo máximo de 15 (quinze) dias, de maneira sincronizada entre as ACs 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.
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 a AC 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 das chaves criptográficas simétricas geradas de forma a garantir a sua preservação, bem como a contingência do sistema de geração e distribuição das chaves, conforme requisitos de segurança definidos na ICP-Brasil.

6. DOCUMENTOS REFERENCIADOS

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