PADRÕES E ALGORITMOS CRIPTOGRÁFICOS

DA ICP-BRASIL (DOC ICP-01.01)

Versão 2.0

18 de agosto de 2008

Sumário

1. INTRODUÇÃO

1.1. Este documento regulamenta os padrões de hardware e os algoritmos e parâmetros criptográficos a serem empregados em todos os processos realizados no âmbito da Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil), que incluem, entre outros:

a) geração de chaves criptográficas;

b) solicitação, emissão e revogação de certificados digitais;

c) geração e verificação de assinaturas digitais;

d) cifração de mensagens;

e) autenticação utilizando certificados digitais.

1.2 A utilização de padrões de hardware e algoritmos criptográficos adequados é essencial para a confiabilidade e credibilidade dos processos que ocorrem na ICP-Brasil.

1.3 As diretrizes aqui constantes devem ser obrigatoriamente observadas pelas Autoridades Certificadoras, Autoridades de Registro, Prestadores de Serviço de Suporte, Empresas de Auditoria Independente, Laboratórios de Ensaio de Auditoria e outras entidades credenciadas ou cadastradas na ICP-Brasil, bem como pelos titulares finais e desenvolvedores de aplicativos que utilizem certificados digitais ICP-Brasil.

1.4 Este documento adota como referência, além das normas da ICP-Brasil, as fontes relacionadas no item 7 – BIBLIOGRAFIA.

2. MOTIVAÇÕES

2.1 A ICP-Brasil instituiu uma infra-estrutura de chaves públicas confiável, em âmbito nacional, com regras e políticas que permitem a emissão e o gerenciamento de certificados digitais para uso em diversas aplicações e processos.

2.2 Para propiciar a segurança adequada aos processos realizados sob o amparo da ICP-Brasil, é necessário que as soluções empregadas acompanhem a evolução tecnológica, pois novos métodos de ataque e o crescimento do poder computacional podem fragilizar processos antes considerados seguros.

2.3 Segundo a MP 2.200, artigo 4º, alínea VIII, estão entre as competências do Comitê Gestor da ICP-Brasil: *"Atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança."*

2.4 Assim, em 07.02.2008 o Comitê Técnico que assessora o Comitê Gestor da ICP-Brasil instituiu o Grupo de Trabalho de Revisão dos Algoritmos Criptográficos da ICP-Brasil, com o objetivo geral de analisar os padrões criptográficos utilizados e propor atualizações, se necessário, dado que os padrões em uso datavam da criação da ICP-Brasil, há seis anos atrás, e não haviam sido revisados desde então.

2.5 O trabalho realizado por aquele GT, nos meses de abril a julho de 2008, contemplou uma proposta de atualização dos algoritmos criptográficos e tamanhos correlacionados de chaves para a ICP-Brasil, levando em consideração uma relação entre o algoritmo criptográfico, o comprimento mínimo de chave, o tempo que um atacante pode quebrar essa segurança e os recursos necessários para obtenção de seu sucesso.

2.6 Suas conclusões, que serviram como base para elaboração da Seção 4 do presente documento, foram calcadas nos trabalhos elaborados pelos seguintes organismos internacionais:

a) NIST - National Institute of Standards and Technology (USA);

b) ETSI - European Telecommunications Standards Institute;

c) CRYPTREC - Cryptography Research and Evaluation Committee (Japão);

d) ECRYPT - European Network of Excellence for Cryptology.

3. DEFINIÇÕES

Para os propósitos deste documento, entende-se por:

3.1. Cifra – É um algoritmo criptográfico utilizado para prover confidencialidade à informação.

3.2. Esquema de Assinatura – conjunto formado por um algoritmo de criação de assinatura, um algoritmo de verificação de assinatura e um algoritmo de geração de chaves, sendo que esse último gera chaves para os outros dois algoritmos.

3.3. Esquema de Envelopes Criptográficos – combinação, formada por uma cifra simétrica e uma cifra assimétrica. Os dados são cifrados com chave simétrica e esta é cifrada com a chave assimétrica pública.

3.4. Função Resumo (*hash*) - é uma transformação matemática que faz o mapeamento de uma seqüência de bits de tamanho arbitrário para uma seqüência de bits de tamanho fixo menor - conhecido como resultado *hash* ou resumo criptográfico - de forma que seja muito difícil encontrar duas mensagens produzindo o mesmo resultado *hash* (resistência à colisão) e que o processo reverso também não seja realizável (dado um resultado *hash*, não é possível recuperar a mensagem que o gerou).

3.5. Método de *Padding* – processo de inserção de bits numa mensagem, preparando-a para a cifração ou assinatura.

3.6 Modo de Operação - Em algoritmos de chaves simétricas, precisamos dividir a mensagem em blocos de tamanho predeterminado antes de passar pelo algoritmo. O modo de operação define o tipo de tratamento que será dado aos blocos de mensagem, para evitar que blocos idênticos gerem o mesmo resultado criptográfico, ao serem cifrados. Esse procedimento visa dar mais segurança ao processo.

3.7 Suíte de assinatura – combinação de um esquema de assinatura com um método de *padding* e uma função resumo.

4. ALGORITMOS E PARÂMETROS CRIPTOGRÁFICOS

Esta Seção relaciona os algoritmos e parâmetros que devem ser utilizados nos procedimentos que envolvem criptografia, no âmbito da ICP-Brasil.

4.1. Funções resumo (*hash*)

Função	Tamanho do *hash*	Referência Normativa
SHA - 1 (*)	160	FIPS 180-2
SHA - 256	256	FIPS 180-2
SHA - 512	512	FIPS 180-2
WHIRLPOOL (**)	512	ISO/IEC 10118-3:2004

(*) Este padrão está citado aqui apenas para fins de compatibilidade com o legado. Novas aplicações não deverão utilizá-lo.

(**) Whirlpool possui princípios de projeto distintos dos da família SHA.

4.2. Métodos de Geração de par de chaves assimétricas

Algoritmo	Algoritmo de Geração de Chaves e Parâmetros	Referência Normativa
RSA	rsagen1	RFC 3447
ECDSA-F_p, ECDH-F_p, ECMQV-F_p	ecgen1	ANSI X9.62
ECDSA-F_{2^m}, ECDH-F_{2^m}, ECMQV-F_{2^m}	ecgen2	ANSI X9.62

4.3. Suítes de Assinaturas

Nome da suíte	Função resumo	Método de *padding*	Algoritmo assinatura	Referência normativa
sha1WithRSAEncryption(*)	SHA1	RSA-PSS with MGF1SHA-1	RSA	PKCS#1 v2.1 RFC 3279
sha256WithRSAEncryption	SHA256	RSA-PSS with MGF1SHA-256	RSA	PKCS#1 v2.1 RFC 4055
sha512WithRSAEncryption	SHA512	RSA-PSS with MGF1SHA-512	RSA	PKCS#1 v2.1 RFC 4055
whirlpoolWithRSAEncryption	WHIRLPOOL	RSA-PSS with MGF1WHIRLPOOL	RSA	PKCS#1 v2.1

sha256WithECDSAEncryption	SHA256	sem *padding*	ECDSA-F_p ou ECDSA-F_2^m	FIPS 186-2 ANSI X9.62
sha512WithECDSAEncryption	SHA512	sem *padding*	ECDSA-F_p ou ECDSA-F_2^m	FIPS 186-2 ANSI X9.62
whirlpoolWithECDSAEncryption	WHIRLPOOL	sem *padding*	ECDSA-F_p ou ECDSA-F_2^m	ISO/IEC 15946-1:2008

(*) Este padrão está citado aqui apenas para fins de compatibilidade com o legado. Novas aplicações não deverão utilizá-lo.

4.4. Algoritmos Simétricos

Função	Referência Normativa
3DES	NIST SP 800-67
AES	ISO/IEC 18033-3 / FIPS 197

4.5. Modos de Operação

Função	Referência Normativa
CBC	NIST SP 800-38A
GCM	NIST SP 800-38D

4.6. Esquemas de Envelopes Criptográficos

Esquema
3desWithRSA2048Encryption
3desWithRSA1024Encryption (*)
aes128WithRSA2048Encryption
aes256WithRSA4096Encryption
aes128WithECDH256Encryption ou ECMQV256Encryption
aes256WithECDH512Encryption ou ECMQV512Encryption

(*) Este padrão está citado aqui apenas para fins de compatibilidade com o legado. Novas aplicações não deverão utilizá-lo.

4.7. Tamanhos de chaves

RSA	Curvas Elípticas	3DES	AES	Período de vida estimado
1024 (*)	--	--	--	1 ano
2048	256	112 (**)	128	10 anos
4096	512	--	256	20 anos

(*) Este padrão está citado aqui apenas para fins de compatibilidade com o legado. Novas aplicações não deverão utilizá-lo.

(**) Mesmo com três chaves distintas de 56 bits (totalizando 168 bits), o nível de segurança do 3DES nunca ultrapassa 112 bits.

4.8. Tamanhos de chaves para assinatura digital

4.8.1 As recomendações que sinalizam a força de algoritmos criptográficos são baseadas nos parâmetros desses algoritmos e são caracterizadas por adotar basicamente comprimentos mínimos de chave, após esses algoritmos terem sido exaustivamente analisados. Essas estimativas de segurança são realizadas levando-se em consideração, principalmente, o esforço computacional necessário para se quebrar um dado algoritmo. Tais estimativas podem ser encontradas na literatura, por exemplo, em LenstraVerheul ou na base de dados do ECRYPT (http://www.ecrypt.eu.org/documents.html).

4.8.2 Não existem provas rigorosas de segurança para os componentes dos sistemas de assinatura (função *hash*, algoritmo de assinatura, RNG). Basicamente, todas as estimativas de segurança dependem de resultados de ataques considerados, atualmente, os mais eficazes. A possibilidade de uma quebra completa de um dado algoritmo (por exemplo, a descoberta de um método rápido de fatoração universal que possa ser usado contra o RSA) em tese não pode ser excluída, mas quebras desse tipo são consideradas como pouco prováveis.

4.8.3 Por outro lado, alguns avanços bastante significativos em análise de algoritmos criptográficos baseados em funções *hash* são considerados como uma ameaça real aos sistemas de assinatura digital. Um exemplo recente são os ataques de colisão ao SHA-1, que demonstraram que essa função *hash* é bastante fraca a esse tipo de ataque.

4.8.4 A margem de segurança para as recomendações abaixo foi escolhida de modo que, mesmo com os avanços tecnológicos, os comprimentos de chave indicados possam garantir a segurança do sistema como um todo. Essa estratégia tem como objetivo evitar problemas graves como, por exemplo, a chave da AC-Raiz ser considerada como insegura de um momento para outro. Além disso, permite um planejamento confiável dos procedimentos de geração e troca de chaves.

4.8.5 Isto significa que, se em 2008, por exemplo, uma chave com um dado comprimento é

considerada como suficientemente segura por 5 anos, ou seja, por pelo menos até o final de 2012, uma futura versão deste documento, uma vez atualizado em 2010, deverá ainda declarar esse comprimento de chave como suficientemente seguro por pelo menos até o final de 2012, se ainda não tiverem sido publicadas quaisquer novas técnicas que provem o contrário.

4.8.6 A tabela a seguir contém recomendações sobre os tempos de uso de suites de assinatura, que foram definidos de acordo com o exposto. Ela relaciona os padrões para algoritmos e parâmetros criptográficos com o tempo de utilização previsto, contado em número de anos, a partir de janeiro de 2008:

Nome da suite de assinatura	**1 ano**	**2 anos**	**5 anos**	**10 anos (especulação)**	**20 anos (especulação)**
sha1WithRSAEncryption (*)	1024	desco-nhecido	Não recomendado		
sha256WithRSAEncryption	1024	1536	2048	2048	4096
sha256WithECDSAEncryption	256	256	256	256	512
sha512WithRSAEncryption	1024	1536	2048	2048	4096
sha512WithECDSAEncryption	256	256	256	256	512
whirlpoolWithRSAEncryption	1024	1536	2048	2048	4096
whirlpoolWithECDSAEncryption	256	256	256	256	512

5. APLICABILIDADE DOS ALGORITMOS E PARÂMETROS CRIPTOGRÁFICOS

Esta Seção relaciona os principais procedimentos que envolvem criptografia, no âmbito da ICP-Brasil, com os algoritmos e parâmetros que devem ser utilizados, **obrigatoriamente**, para sua execução, e também com os documentos normativos que tratam desses procedimentos.

Solicitação de certificados à AC	
Normativo ICP-Brasil	DOC-ICP-01 - item 4.1.2 DOC-ICP-01 - item 6.1.3.1 DOC-ICP-04 - item 6.1.3 DOC-ICP-05 - item 4.1.3
Formato	Padrão PKCS#10

Entrega de certificados emitidos pela AC	
Normativo ICP-Brasil	DOC-ICP-01 - item 4.2.4 DOC-ICP-01 - item 6.1.4.1 DOC-ICP-04 - item 6.1.4 DOC-ICP-05 - item 6.1.4
Formato	Padrão PKCS#7

Geração de chaves assimétricas de AC	
Normativo ICP-Brasil	DOC-ICP-01 - item 6.1.1.3 DOC-ICP-04 - item 6.1.1.3 DOC-ICP-01 - item 6.1.5 DOC-ICP-05 - item 6.1.5
Algoritmo	RSA, ECDSA-F_p, ECDSA-F_{2^m}
Tamanho de chave	RSA 2048(*), RSA 4096, ECDSA 512

(*) *Este padrão está citado aqui apenas para fins de compatibilidade com o legado. Novas aplicações não deverão utilizá-lo.*

Geração de chaves assimétricas de usuário final	
Normativo ICP-Brasil	DOC-ICP-04 - item 6.1.5.2
Algoritmo	RSA, ECDSA-F_p, ECDSA-F_{2^m}
Tamanho da chave A1, A2, A3, S1, S2, S3, T3	RSA 1024(*), RSA 2048, ECDSA 256
Tamanho da chave A4, S4, T4	RSA 2048(*), RSA 4096, ECDSA 512

(*) *Este padrão está citado aqui apenas para fins de compatibilidade com o legado. Novas aplicações não deverão utilizá-lo.*

Assinatura de certificados de AC	
Normativo ICP-Brasil	DOC-ICP-01 - item 7.1.3 DOC-ICP-01 - item 7.2.3 DOC-ICP-05 - item 7.2.3
Suite de Assinatura	sha1WithRSAEncryption(*) sha512WithRSAEncryption whirlpoolWithRSAEncryption sha512WithECDSAEncryption whirlpoolWithECDSAEncryption

(*) *Este padrão está citado aqui apenas para fins de compatibilidade com o legado. Novas aplicações não deverão utilizá-lo.*

Assinatura de certificados de usuário final	
Normativo ICP-Brasil	DOC-ICP-04 - item 7.1.3
Suíte de Assinatura	sha1WithRSAEncryption(*) sha512WithRSAEncryption whirlpoolWithRSAEncryption sha512WithECDSAEncryption whirlpoolWithECDSAEncryption

(*) *Este padrão está citado aqui apenas para fins de compatibilidade com o legado. Novas aplicações não deverão utilizá-lo.*

Assinatura de Listas de Certificados Revogados e Respostas OCSP	
Normativo ICP-Brasil	DOC-ICP-01 - item 7.3 DOC-ICP-04 - item 7.2 DOC-ICP-05 - item 7.3
Algoritmo de Assinatura	sha1WithRSAEncryption(*) sha512WithRSAEncryption

	whirlpoolWithRSAEncryption sha512WithECDSAEncryption whirlpoolWithECDSAEncryption

(*) *Este padrão está citado aqui apenas para fins de compatibilidade com o legado. Novas aplicações não deverão utilizá-lo.*

Guarda da chave privada da entidade titular e de seu *backup*	
Normativo ICP-Brasil	DOC-ICP-04 - item 6.1.1.3 DOC-ICP-04 - item 6.2.4.3 DOC-ICP-05 - item 6.2.4.4
Algoritmo e Tamanho de chave	3DES – 112 bits AES – 128 ou 256 bits
Modo de operação	CBC ou GCM

Assinaturas digitais ICP-Brasil CaDES e XaDES (*)	
Normativo ICP-Brasil	DOC-ICP-15, item 6.1
Função resumo	SHA - 1 (**) SHA - 256 SHA - 512 WHIRLPOOL
Suíte de Assinatura	Sha1WithRSAEncryption (**) sha256WithRSAEncryption sha512WithRSAEncryption whirlpoolWithRSAEncryption sha256WithECDSAEncryption sha512WithECDSAEncryption whirlpoolWithECDSAEncryption

(*) Uma assinatura digital ICP-Brasil contém um identificador da função resumo que está sendo usada e um identificador do algoritmo de assinatura que está sendo usado, o qual precisa estar consistente com o identificador do algoritmo de assinatura contido no certificado do signatário. Os requisitos aplicam-se tanto à função resumo como ao algoritmo de assinatura.

(**) Este padrão está citado aqui apenas para fins de compatibilidade com o legado. Novas aplicações não deverão utilizá-lo.

Assinatura de Pedidos e Respostas de Carimbos do Tempo	
Normativo ICP-Brasil	DOC-ICP-12, item 7.2
Função resumo	SHA - 1 (*) SHA - 256 SHA - 512 WHIRLPOOL
Suíte de Assinatura	Sha1WithRSAEncryption (*) sha256WithRSAEncryption sha512WithRSAEncryption whirlpoolWithRSAEncryption sha256WithECDSAEncryption sha512WithECDSAEncryption whirlpoolWithECDSAEncryption

(*) Este padrão está citado aqui apenas para fins de compatibilidade com o legado. Novas aplicações não deverão utilizá-lo.

6. PADRÕES DE HARDWARE

A tabela a seguir relaciona os padrões a serem empregados nos hardwares criptográficos com sua utilização na ICP-Brasil e com os documentos normativos que tratam dessa utilização.

Utilização	Padrões	Normativo
Módulo criptográfico de geração de geração de chaves assimétricas de usuário final	Padrão FIPS 140-**2**	DOC-ICP-04 - item 6.2.1 DOC-ICP-05 - item 6.2.1.2
Módulo criptográfico para armazenamento da chave privada de titular do certificado	Padrão FIPS 140-**2**	DOC-ICP-04 - item 6.8
Parâmetros de geração de chaves assimétricas de usuário final	Padrão FIPS 140-**2**	DOC-ICP-04 - item 6.1.6
Módulo criptográfico de geração de chaves assimétricas de AC	Padrão FIPS 140-**2** *level 2*	DOC-ICP-05 - item 6.2.1.1
Módulo criptográfico para armazenamento da chave privada de AC	Padrão FIPS 140-**2** *level 2*	DOC-ICP-05 - item 6.8
Parâmetros de geração de chaves assimétricas de AC	Padrão FIPS 140-**2** *level 2*	DOC-ICP-05 - item 6.1.6
Módulo criptográfico de geração de chaves assimétricas da AC Raiz	Padrão FIPS 140-**2** *level 3*	DOC-ICP-01- item 6.2.1
Módulo criptográfico para armazenamento da chave privada da AC Raiz	Padrão FIPS 140-**2** *level 3*	DOC-ICP-01- item 6.8
Parâmetros de geração de chaves assimétricas da AC Raiz	Padrão FIPS 140-**2** *level 3*	DOC-ICP-01- item 6.1.6
Processo para verificação de parâmetros de geração de chaves assimétricas	Processo de Homologação da ICP-Brasil	DOC-ICP-01 - item 6.1.7 DOC-ICP-04 - item 6.1.7 DOC-ICP-05 - item 6.1.7

6. DOCUMENTOS REFERENCIADOS

Os documentos abaixo são aprovados por Resolução do Comitê-Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio http://www.iti.gov.br publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Código	Nome do documento
DOC-ICP-01	DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AUTORIDADE CERTIFICADORA RAIZ DA ICP-BRASIL
DOC-ICP-04	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL
DOC-ICP-05	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DE CERTIFICAÇÃO DAS AUTORIDADES CERTIFICADORAS DA ICP-BRASIL
DOC-ICP-12	REQUISITOS MÍNIMOS PARA AS DECLARAÇÕES DE PRÁTICAS DAS AUTORIDADES DE CARIMBO DO TEMPO DA ICP-BRASIL (documento em fase de aprovação)
DOC-ICP-15	ASSINATURAS DIGITAIS NA ICP-BRASIL (documento em fase de aprovação)

7. BIBLIOGRAFIA

Jonsson, J. and Kaliski, B. 2003 Public-Key Cryptography Standards (Pkcs) #1: RSA Cryptography Specifications Version 2.1. RFC. RFC Editor.

ANSI X9.62. Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005.

National Institute of Standards and Technology, Federal Information Processing Standards Publication 186-2: Digital Signature Standard. Janeiro 2000.

IEEE Standard 1363--2000. Standard Specifications for Public Key Cryptography. IEEE Standards Organization, 2000.

ISO/IEC-15946-1:2008, Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 1: General, International Standards Organization, 2008.

ISO/IEC-15946-3, Information Technology-Security Techniques - -Cryptographic Techniques based on Elliptic Curves-Part 3: Key Establishment, International Standards Organization, 2002.

SECG, Elliptic Curve Cryptography, Standards for Efficient Cryptography Group, 2000.

SECG, Recommended Elliptic Curve Domain Parameters, Standards for Efficient Cryptography Group, 2000.

PKCS #3: Diffie-Hellman Key-Agreement Standard, RSA Laboratories, Redwood City, California, Novembro 1993

National Institute of Standards and Technology, Federal Information Processing Standards Publication 180-2: Secure Hash Standard. Agosto 2002.

ISO 10118 - 3, Information technology - Security techniques - Hash-functions, Part 3: Dedicated hash-functions, 2004

National Institute of Standards and Technology, Federal Information Processing Standards Publication 197: Advanced Encryption Standard (AES). Novembro 2001.

Anderson, Biham, Knudsen, Serpent: A Proposal for the Advanced Encryption Standard,

First Advanced Encryption Standard (AES) Conference, EUA, 1998.

NIST Pub 800-38A 2001 ED, Recommendation for Block Cipher Modes of Operation - Methods and Techniques, NIST Special Publication 800-38A, US Department of Commerce/N.I.S.T., Dezembro 2001.

Kalle Kaukonen and Rodney Thayer. A stream cipher encryption algorithm "arcfour". Internet draft (draft-kaukonencipher-arcfour-03), Network Working Group, Julho 1999.

National Institute of Standards and Technology, Federal Information Processing Standards Publication 198: The Keyed-Hash Message Authentication Code (HMAC). Março 2002.

NIST Pub 800-38A 2001 ED, Recommendation for Block Cipher Modes of Operation - The CMAC Mode for Authentication, NIST Special Publication 800-38B, US Department of Commerce/N.I.S.T., Março 2005.

ETSI. Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms; ETSI TR 102 176-1A (2007-11); European Telecomunications Standards Institute, 2007.