DIÁRIO OFICIAL DA UNIÃO

Publicado em: 17/09/2021 | Edição: 177 | Seção: 1 | Página: 9

Órgão: Presidência da República/Casa Civil/Instituto Nacional de Tecnologia da Informação

PORTARIA CONJUNTA ITI/CC/PR SGD/SEDGG/ME Nº 1, DE 8 DE SETEMBRO DE 2021

Estabelece os padrões criptográficos referenciais para as assinaturas eletrônicas avançadas nas comunicações que envolvam a administração pública federal direta, autárquica e fundacional.

O DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO e o SECRETÁRIO DE GOVERNO DIGITAL DA SECRETARIA ESPECIAL DE DESBUROCRATIZAÇÃO, GESTÃO E GOVERNO DIGITAL DO MINISTÉRIO DA ECONOMIA , no uso das atribuições que lhes conferem o inciso I do art. 9º do Decreto nº 10.543, de 13 de novembro de 2020, resolvem:

Art. 1º Aprovar, na forma prevista no Anexo I desta Portaria, os padrões criptográficos referenciais para as assinaturas eletrônicas avançadas nas comunicações que envolvam a administração pública federal direta, autárquica e fundacional.

§ 1º Os padrões criptográficos previstos nesta portaria são de observância obrigatória nos casos de uso de assinaturas eletrônicas avançadas nas comunicações e iterações envolvendo entes ou entidades da Administração Federal direta, autárquica e fundacional, entre si ou com pessoas naturais ou entes e entidades de direito privado.

§ 2º Os padrões aprovados nocaputpoderão ser revistos ou atualizados por meio de portaria conjunta, a qualquer momento, em razão dos avanços tecnológicos em criptografia e assinaturas eletrônicas.

Art. 2º Esta Portaria entra em vigor no dia 1º de outubro de 2021.

CARLOS ROBERTO FORTNER
Diretor-Presidente do Instituto Nacional
de Tecnologia da Informação

LUIS FELIPE SALIN MONTEIRO
Secretário de Governo Digital

ANEXO

1. INTRODUÇÃO

1.1 Este regulamento estabelece os padrões referenciais de hardware, algoritmos e parâmetros criptográficos a serem empregados nos processos que envolvem a realização de assinaturas eletrônicas avançadas, compreendendo:

a) geração de chaves criptográficas;

b) solicitação, emissão e revogação de certificados digitais avançados;

c) geração e verificação de assinaturas eletrônicas avançadas;

d) cifração de mensagens;

e) autenticação com certificados digitais avançados.

1.2. As diretrizes aqui constantes devem ser obrigatoriamente observadas por órgãos e entidades, públicos e privados, provedores de serviços de emissão de certificados digitais avançados e de aplicações que realizem e verifiquem assinaturas eletrônicas avançadas.

2. ALGORITMOS E PARÂMETROS CRIPTOGRÁFICOS

2.1. Solicitação de certificado digital avançado à Autoridade Certificadora emissora:

2.1.1. Formato Padrão PKCS#10

2.2. Entrega de certificado digital avançado emitido pela Autoridade Certificadora:

2.2.1. Formato Padrão PKCS#7

2.3 Geração de chaves criptográficas assimétricas de Autoridade Certificadora emissora de certificados digitais avançados:

2.3.1. Algoritmos admitidos:

a) RSA;

b) ECC-Brainpool (conforme RFC 5639);

c) Ed448-Goldilocks (PureEdDSA e HashEdDSA, conforme RFC 8032);

d) E-521 (Conforme parâmetros da curva estabelecidos no item 2.13, PureEdDSA e HashEdDSA, conforme RFC 8032).

2.3.2 Tamanhos de Chaves admitidos:

a) RSA - 4096 bits;

b) ECC-Brainpool - 512 bits (curva P512r1);

c) Ed448-Goldilocks - 448 bits;

d) E-521 - 521 bits.

2.4. Geração de chaves criptográficas assimétricas de usuário final de certificados digitais avançados:

2.4.1. Algoritmos admitidos:

a) RSA;

b) ECC-Brainpool (conforme RFC 5639);

c) Curve25519 (conforme RFC 7748);

d) Ed25519 (PureEdDSA e HashEdDSA, conforme RFC 8032);

e) Ed448-Goldilocks (PureEdDSA e HashEdDSA, conforme RFC 8032);

f) E-521 (Conforme parâmetros da curva estabelecidos no item 2.13, PureEdDSA e HashEdDSA, conforme RFC 8032).

2.4.2. Tamanhos de Chaves admitidos:

a) RSA - 2048 e 4096 bits;

b) ECC-Brainpool - 256 e 512 bits (curvas P256r1 e P512r1, respectivamente);

c) Curve25519 - 256 bits;

d) Ed25519 - 256 bits;

e) Ed448-Goldilocks - 448 bits;

f) E-521 - 521 bits.

2.5. Assinatura de certificados de Autoridades Certificadoras emissoras de certificados digitais avançados:

2.5.1 Suítes de assinatura admitidas:

a) sha512WithRSAEncryption;

b) sha512WithECDSAEncryption;

c) sha3-512WithRSAEncryption;

d) sha3-512WithECDSAEncryption;

e) id-Ed448;

f) id-Ed448ph;

g) id-Ed521;

h) id-Ed521ph.

2.6. Assinatura de certificados avançados de usuários finais:

2.6.1. Suítes de assinatura admitidas:

a) sha256WithRSAEncryption;

b) sha3-256WithRSAEncryption;

c) sha256WithECDSAEncryption;

d) sha3-256WithECDSAEncryption;

e) sha512WithRSAEncryption;

f) sha3-512WithRSAEncryption;

g) sha512WithECDSAEncryption;

h) sha3-512WithECDSAEncryption;

i) id-Ed25519;

j) id-Ed25519ph;

k) id-Ed448;

l) id-Ed448ph;

m) id-Ed521;

n) id-Ed521ph.

2.7. Assinatura de listas de certificados avançados revogados e de respostas OCSP:

2.7.1 Suítes de assinatura admitidas:

a) sha256WithRSAEncryption;

b) sha3-256WithRSAEncryption;

c) sha256WithECDSAEncryption;

d) sha3-256WithECDSAEncryption;

e) sha512WithRSAEncryption;

f) sha3-512WithRSAEncryption;

g) sha512WithECDSAEncryption;

h) sha3-512WithECDSAEncryption;

i) id-Ed448;

j) id-Ed448ph;

k) id-Ed521;

l) id-Ed521ph.

2.8. Guarda de chaves criptográficas privadas de entidades titulares e de seus backups:

2.8.1 Algoritmos e tamanhos de chaves admitidos:

a) AES - 128 ou 256 bits;

b) Serpent - 128 e 256 bits.

2.8.2. Modos de operação admitidos:

a) GCM.

2.9.1. Funções resumo (Hash) admitidas:

a) SHA-256;

b) SHA-512;

c) SHAKE - 256;

d) SHA3-256;

e) SHA3-512.

2.9.2. Suítes de assinatura admitidas:

a) sha256WithRSAEncryption;

b) sha3-256WithRSAEncryption;

c) sha256WithECDSAEncryption;

d) sha3-256WithECDSAEncryption;

e) sha512WithRSAEncryption;

f) sha3-512WithRSAEncryption;

g) sha512WithECDSAEncryption;

h) sha3-512WithECDSAEncryption;

i) id-Ed25519;

j) id-Ed25519ph;

k) id-Ed448;

l) id-Ed448ph;

m) id-Ed521;

n) id-Ed521ph.

2.10. Assinatura de pedidos e respostas de Carimbos do Tempo:

2.10.1. Funções resumo (Hash) admitidas:

a) SHA-256;

b) SHA-512;

c) SHAKE - 256;

d) SHA3-256;

e) SHA3-512.

2.10.2. Suítes de assinatura admitidas:

a) sha256WithRSAEncryption;

b) sha3-256WithRSAEncryption;

c) sha256WithECDSAEncryption;

d) sha3-256WithECDSAEncryption;

e) sha512WithRSAEncryption;

f) sha3-512WithRSAEncryption;

g) sha512WithECDSAEncryption;

h) sha3-512WithECDSAEncryption;

i) id-Ed25519;

j) id-Ed25519ph;

k) id-Ed448;

l) id-Ed448ph

m) id-Ed521;

n) id-Ed521ph.

2.11. Esquemas de acordos de chaves criptográficas admitidos:

a) ECDH256 ou ECMQV256;

b) ECDH512 ou ECMQV512;

c) ECDHE X25519;

d) ECDHE X448;

e) RSA 2048;

f) RSA 4096.

2.12. Esquemas de envelopes criptográficos admitidos:

a) aes128WithRSA2048Encryption;

b) aes256WithRSA4096Encryption;

c) aes128WithECIES256Encryption;

d) aes256WithECIES512Encryption.

2.13. Parâmetros para a curva E-521:

2.13.1 Tabela de parâmetros e valores correspondentes:

Parâmetros	Valor
p	P da E-521(i.e.,2^521 - 1)
b	528
Codificação do GF(p)	527-bit codificação litlle-endian de {0,1...,p-1}
H(x)	SHAKE256(dom5(phflag,context)||x, 132)
phflag	0
c	Logaritmo base 2 do cofator da E-521(i.e.,2)
n	520
d	D da E-521(i.e., - 376014)
a	1
B	(X(P),Y(P)) da E-521 (i.e., (15710548 941849953875359397498943175686452973504029058214376251811523049943811885296325911960676041007726739279151142671933899050032766737490120511483560413 24, 12))
L	ordem da E-521 (i.e., 1716199415032652428745475199770348304317358825035826352348615864796385795849413675475876651663657849636693659065234142604319282948702542317993421293670108523)
PH (X)	x (i.e., a função identidade)

2.13.2. Ed521ph é o mesmo, mas com PH sendo SHA-3 (512 bits) ou SHAKE256(x, 64) e phflag sendo 1, i.e., é feito um hash antes da assinatura com Ed521, com a constante hash modificada.

2.13.3. dom5(x, y): na geração de chave, uma string vazia. Na assinatura e verificação, a string do octeto "SigEd521" || octet(x) || octet(OLEN(y)) || y, onde x está no range 0-255 e y é uma string de octeto com no máximo 255 octetos. "SigEd521" está em ASCII (8 octets).

3. PADRÕES DE HARDWARE

3.1. Módulo criptográfico (HSM) de parametrização, geração e armazenamento de chaves criptográficas assimétricas de usuários finais de certificados digitais avançados em nuvem:

3.1.1. Este requisito se aplica somente para o caso de geração e armazenamento das chaves criptográficas de usuário final pela AC emissora do certificado digital avançado;

3.1.2. NSH-2 - Homologação ICP-Brasil, ou Certificação INMETRO, ou FIPS 140-2 nível 3, ou Common Criteria EAL 4+ eiDAS Protection Profile EN-419-221-5.

3.2. Módulo criptográfico (HSM) de parametrização, geração e armazenamento de chaves criptográficas assimétricas de Autoridade Certificadora emissora de certificados digitais avançados:

3.2.1. NSH-2 - Homologação ICP-Brasil, ou Certificação INMETRO, ou FIPS 140-2 nível 3, ou Common Criteria EAL 4+ eiDAS Protection Profile EN-419-221-5.

3.3. Módulo criptográfico (HSM) de parametrização, geração e armazenamento de chaves criptográficas assimétricas de Autoridade Certificadora Raiz de infraestrutura para emissão de certificados digitais avançados:

3.3.1. NSH-3 - Homologação ICP-Brasil, ou Certificação INMETRO, ou FIPS 140-2 nível 3, ou Common Criteria EAL 4+ eiDAS Protection Profile EN-419-221-5.

4. PERFIL DE CERTIFICADOS

4.1. Perfil de Certificado: em conformidade com o formato definido pelo padrão ITU X.509 ou ISO/IEC 9594-8, de acordo com o perfil estabelecido na RFC 5280;

4.2. Número da versão do certificado: versão 3 de certificado definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280;

4.3. Extensões de certificado obrigatórias:

4.3.1. Certificados de AC:

4.3.1.1.*Authority Key Identifier*, não crítica: deve conter o hash SHA-256 da chave pública da AC que emite o certificado;

4.3.1.2.*Subject Key Identifier*, não crítica: deve conter o hash SHA-256 da chave pública da AC titular do certificado;

4.3.1.3.*Key Usage*, crítica: somente os bits keyCertSign e cRLSign devem estar ativados;

4.3.1.4.*Certificate Policies*, não crítica:

4.3.1.4.1. O campo policyIdentifier deve conter:

4.3.1.4.1.1. O OID da DPC da AC titular do certificado, se essa AC emite certificados para outras ACs; ou

4.3.1.4.1.2. Os OID das PCs que a AC titular do certificado implementa, se essa AC emite certificados para usuários finais;

4.3.1.4.2. O campo policyQualifiers deve conter o endereço Web da DPC da AC que emite o certificado;

4.3.1.5.*Basic Constraints*, crítica: deve conter o campo cA=True; e

4.3.1.6.*CRL Distribution Points*, não crítica: deve conter o endereço na Web onde se obtém a LCR correspondente ao certificado.

4.3.2. Certificados de usuário final:

4.3.2.1.*Authority Key Identifier*, não crítica: deve conter o hash SHA-256 da chave pública da AC que emite o certificado;

4.3.2.2.*Key Usage*, crítica: deve conter o bit digitalSignature ativado, podendo conter os bits keyEncipherment e nonRepudiation ativados;

4.3.2.3.*Extended Key Usage*, não crítica: no mínimo um dos propósitos client authentication (OID = 1.3.6.1.5.5.7.3.2) ou E-mail protection (OID = 1.3.6.1.5.5.7.3.4) deve estar ativado;

4.3.2.4.*Certificate Policies*, não crítica: deve conter o OID da PC correspondente e o endereço Web da DPC da AC que emite o certificado;

4.3.2.5.*CRL Distribution Points*, não crítica: deve conter o(s) endereço(s) na Web onde se obtém a LCR correspondente;

4.3.2.6.*Authority Information Access*, não crítica: A primeira entrada deve conter o método de acesso id-ad-caIssuer, utilizando um dos seguintes protocolos de acesso, HTTP, HTTPS ou LDAP, para a recuperação da cadeia de certificação. A segunda entrada deve conter o método de acesso id-ad-ocsp, com o respectivo endereço do respondedor OCSP, quando implementado, utilizando um dos seguintes protocolos de acesso, HTTP, HTTPS ou LDAP;

4.3.2.7.*Subject Alternative Name*, não crítica, e com os seguintes formatos:

4.3.2.7.1. Para certificados de pessoas físicas:

4.3.2.7.1.1. Campo*otherName*, obrigatório, contendo OID = 2.16.76.1.3.1 e conteúdo = nas primeiras 8 (oito) posições, a data de nascimento do titular, no formato ddmmaaaa; nas 11 (onze) posições subsequentes, o Cadastro de Pessoa Física (CPF) do titular;

4.3.2.7.2. O conjunto de informações definido em cada campo*otherName*deve ser armazenado como uma cadeia de caracteres do tipo ASN.1 OCTET STRING ou PRINTABLE STRING;

4.3.2.7.3. Apenas os caracteres de A a Z, de 0 a 9, poderão ser utilizados, não sendo permitidos os demais caracteres especiais;

4.4. Formato de Nome: O nome do titular do certificado, constante do campo "*Subject*", deverá adotar o "*Distinguished Name*" (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

O = GOV-BR

OU = nome da AC emissora do certificado

CN = (i) se certificado de AC = nome da AC titular do certificado; (ii) se certificado de pessoa física = nome do titular do certificado

4.5. São aplicáveis as seguintes restrições para os nomes de titulares de certificados:

4.5.1. não deverão ser utilizados sinais de acentuação, tremas ou cedilhas; e

4.5.2. além dos caracteres alfanuméricos, poderão ser utilizados somente os seguintes caracteres especiais:

Caractere	Código NBR9611 (hexadecimal)
Branco	20
!	21
"	22
#	23
$	24
%	25
&	26
'	27
(	28
)	29
*	2A
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

5. PERFIL DE LCR

5.1. Número de versão de LCR: versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280;

5.2. Extensões obrigatórias de LCR:

5.2.1.*Authority Key Identifier*, não crítica: deve conter o hash SHA-256 da chave pública da AC que assina a LCR; e

5.2.2.*CRL Number*, não crítica: deve conter um número sequencial para cada LCR emitida pela AC;

5.2.3. Frequência de emissão de LCR:

5.2.3.1. Nos casos de AC Raiz e AC Intermediária, no máximo a cada 90 dias;

5.2.3.2. No caso de AC final, no máximo a cada hora (60 minutos).

6. PERFIL DE OSCP

6.1. Número de versão de OSCP: serviços de respostas OCSP deverão implementar a versão 1 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 6960;

6.2. Extensões de OSCP: se implementado, deve estar em conformidade com a RFC 6960.

7. PADRÕES DE FORMATOS DE ASSINATURAS ELETRÔNICAS AVANÇADAS:

7.1. Padrão CAdES (CMS*Advanced Electronic Signature*), conforme definido pela ETSI TS 101 733;

7.2. Padrão XAdES (XML*Advanced Electronic Signature*), conforme definido pela ETSI TS 101 903 e TS 103 171; e

7.3. Padrão PAdES (PDF*Advanced Electronic Signature)*, conforme definido pela ETSI TS 102 778.

8. REQUISITOS GERAIS

8.1. Para a emissão de certificado digital avançado, a identificação do titular do certificado deverá ser comprovada por validador de acesso digital cadastrado pela SGD/ME, conforme regulamento editado por aquela Secretaria.

8.2. Disponibilidade de serviços: as entidades provedoras de certificados digitais avançados devem declarar qual a disponibilidade dos seus serviços.

8.2.1. A disponibilidade recomendada é de, no mínimo, 99,5% (noventa e nove vírgula cinco por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

8.2.2. É responsabilidade do provedor dos serviços publicar regularmente a disponibilidade de seus serviços para conhecimento público.

8.3. As entidades provedoras de certificados digitais avançados devem dispor em suas Declarações de Práticas de Certificação (DPC) e Políticas de Certificados (PC) a conformidade aos parâmetros estabelecidos por este regulamento, bem como os demais que regem suas operações, em conformidade à RFC 3642 da IETF.

8.3.1. As DPCs e PCs referidas no item anterior devem estar publicadas para livre acesso e conhecimento da sociedade em geral.

8.4. Os provedores de serviços de emissão de certificados digitais avançados e de aplicações que realizem e verifiquem assinaturas eletrônicas avançadas deverão solicitar à SGD integração de seus serviços à Plataforma Gov.br.

8.5. Para garantir o reconhecimento das cadeias de confiança envolvidas e a interoperabilidade das assinaturas eletrônicas avançadas, o ITI manterá uma Lista de Serviços de Assinaturas Eletrônicas Avançadas integrados à Plataforma Gov.br, a partir da informação de integração repassada pela SGD.

8.6. Para efeito do disposto no item anterior o ITI poderá avaliar as DPCs, PCs e certificados envolvidos na cadeia de confiança do provedor de certificados digitais avançados, bem como, amostras de documentos com assinaturas eletrônicas avançadas dos provedores de aplicações que realizem e verifiquem assinaturas eletrônicas avançadas.

8.7. A qualquer tempo, ao tomar conhecimento da ocorrência de irregularidades nos serviços prestados pelos provedores incluídos na Lista de Serviços de Assinaturas Eletrônicas Avançadas integrados à Plataforma Gov.br, a SGD solicitará ao ITI a exclusão do provedor correspondente da lista.

8.8. Os serviços incluídos na Lista de Serviços de Assinaturas Eletrônicas Avançadas integrados à Plataforma Gov.br são de responsabilidade exclusiva de seus provedores, respondendo por eventuais danos a que derem causa. A SGD e o ITI não se responsabilizam pelos mesmos sob qualquer hipótese. A

referida lista tem por objetivo apenas dar publicidade aos serviços dela constantes e prover interoperabilidade dos documentos digitais assinados através desses serviços.

8.9. No caso de haver necessidade de inclusão de informações adicionais (opcionais) nos certificados digitais avançados, o ITI deverá ser consultado e, se for o caso, atribuirá um OID específico para o caso.