PORTARIA Nº 68, DE 20 DE NOVEMBRO DE 2019.

Estabelece o padrão nacional de certificação digital a ser utilizado na Carteira de Identificação Estudantil

O DIRETOR PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO - ITI, autarquia federal vinculada à Casa Civil da Presidência da República, em cumprimento à Lei Federal nº 12.933, de 26 de dezembro de 2013, que trata, do benefício da meia-entrada em espetáculos artístico-culturais e esportivos,

CONSIDERANDO que, nos termos do art. 1°-A, §2° e §3°, da Lei n° 12.933, de 26 de dezembro de 2013, incluído pela Medida Provisória n° 895, de 6 de setembro de 2019, a Carteira de Identificação Estudantil, em padronização a ser definida pelo Ministério da Educação, deverá contar com certificação digital do Instituto Nacional de Tecnologia da Informação - ITI, provida pela Infraestrutura de Chaves Pública Brasileira – ICP-Brasil;

CONSIDERANDO que o Ministério da Educação editou a Portaria nº 1.773, de 18 de outubro de 2019, dispondo sobre as diretrizes para formação do cadastro do Sistema Educacional Brasileiro - SEB e expedição da Carteira de Identificação Estudantil;

CONSIDERANDO que, consoante o art. 13 da Medida Provisória n° 2.200-2, de 24 de agosto de 2001, o Instituto Nacional de Tecnologia da Informação – ITI é a Autoridade Certificadora Raiz da ICP-Brasil;

RESOLVE:

Art. 1º Esta Portaria estabelece o padrão nacional de certificação digital a ser utilizado na Carteira de Identificação Estudantil, nos termos do art. 1°-A, §§2° e 3°, da Lei 12.933, de 2013, incluído pela Medida Provisória nº 895, de 2019.

Parágrafo único. As especificações estão dispostas no documento em anexo “Certificação de Atributo referente à Carteira de Identificação Estudantil (CACIE) – Versão 3.0”, que se encontra disponibilizado no seguinte endereço eletrônico: www.iti.gov.br.

Art. 2º Os certificados de atributos associados às Carteiras de Identificação Estudantil emitidas até a data da entrada em vigor desta Portaria, de acordo com o padrão nacional fixado pela Portaria nº 78, de 2018, permanecerão válidas até 31 de março de 2020.

Art. 3º Fica revogada a Portaria nº 78, de 24 de dezembro de 2018.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

MARCELO AMARO BUZ

Assinado de forma digital por MARCELO AMARO BUZ
Dados: 2019.11.20 17:00:07 -03'00'

Marcelo Amaro Buz
Diretor-Presidente

Anexo I

Certificação de Atributo referente à Carteira de Identificação Estudantil (CACIE)

(Art. 1º-A, § 1ºe §2º da Lei nº 12.933, de 26/12/2013 e MP 895/19)

Versão 3.0

LISTA DE SIGLAS e ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AR	Autoridade de Registro
A3/A4	Certificado Digital de Assinatura (tipo 3 ou tipo 4)
CIE	Carteira de Identificação Estudantil
DOC-ICP-16	Documento de Padronização do Certificado de Atributo da ICP-Brasil
CA	Certificado de Atributo
EEA	Entidade Emissora de Atributos
ICP-Brasil	Infraestrutura de Chaves Públicas Brasileira
ITI	Instituto Nacional de Tecnologia da Informação
LCAR	Lista de Certificados de Atributos Revogados

1. Introdução

A Carteira de Identificação Estudantil (CIE) é um documento de modelo único nacionalmente padronizado conforme estabelecido pela Lei 12.933/13 e Medida Provisória nº 895/19.

Ao Instituto Nacional de Tecnologia da Informação (ITI) conforme Art.1º-A §1 e §2 da Lei nº 12.933/13; cabe definir as características técnicas associadas a certificação digital padrão ICP-Brasil.

A tecnologia utilizada para suportar o uso da certificação digital, conforme estabelecido na legislação da ICP-Brasil, é o certificado de atributo. O certificado de atributo é um documento eletrônico assinado por um certificado digital de uma entidade emissora cujo objetivo é atestar a qualificação de um cidadão, neste caso, se é estudante. As informações constantes num certificado de atributo associado a CIE permite a validação eletrônica de forma segura da situação de estudante.

O Certificado de Atributo é uma das tecnologias disponíveis a partir do sistema de Certificação Digital padrão ICP-Brasil, padronizado pelo DOC-ICP-16 e DOC-ICP-16.01.

2. Especificação do Certificado de Atributo da CIE

O formato digital da CIE será implementado por meio do uso de certificado de atributo (DOC-ICP-16), do tipo autônomo, conforme regulamento da ICP-Brasil.

Os documentos técnicos DOC-ICP-16 e DOC-ICP-16.01, definem o perfil do certificado de atributo com os campos apresentados na Tabela I, com as descrições a seguir.

Seq.	Campo	
1	Versão	version v2(1)
2	Titular do Certificado de Atributo	holder
3	Emissor	issuer
4	Algoritmo de Assinatura	signature
5	Número de Série	serialNumber
6	Período de Validade	attCertValidityPeriod
7	Atributos	attributes
8	Extensões	extensions
9	Assinatura Digital	SignatureValue

Tabela I – conteúdo do Certificado de Atributo

2.1. Versão

Deve ser adotada a versão v2, representado pelo valor inteiro (1).

2.2. Titular do Certificado de Atributo

O nome do titular do certificado de atributo, pessoa física, constante no campo *Holder*, deverá adotar o *Distinguished Name* (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C = BR

O = ICP-Brasil

OU = nome de fantasia ou sigla da Entidade Emissora de Atributo (EEA)

CN = nome do titular do atributo

Na composição dos nomes, aplicam-se as restrições de nome conforme definido no item 2.4 deste documento.

2.3 Emissor do Certificado de Atributo

O nome da entidade emissora do certificado de atributo, pessoa jurídica, constante no campo *Issuer*, deverá adotar o *Distinguished Name* (DN) do padrão ITU X.500/ISO 9594, no mesmo formato de codificação e conteúdo do campo *Subject* do certificado da signatária do certificado de atributo (EEA).

2.4 Restrição de nomes

Na composição de nomes, aplicam-se as seguintes restrições:

a) não deverão ser utilizados sinais de acentuação, tremas ou cedilhas; e

b) além dos caracteres alfanuméricos, poderão ser utilizados somente os caracteres especiais apresentados na Tabela II.

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

Tabela II - Caracteres especiais admitidos na descrição de nomes

2.5 Algoritmo de Assinatura

Contém o identificador do algoritmo utilizado para validar a assinatura do Certificado de Atributo. Este algoritmo deve ser um dos algoritmos de assinatura de certificados de usuário final definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL (DOC-ICP-01.01).

2.6 Número de Série

Este campo deve possuir o par *issuer/serialNumber* ÚNICO. O campo *serialNumber* deve ser um número inteiro e positivo com um limite máximo de até 20 octetos.

2.7 Período de Vigência

O campo período de vigência deve possuir o formato *GeneralizedTime*, padrão ASN.1 e expresso em UTC (*Universal Time Coordinated*) AAAAMMDDHHMMSSZ.

O período de vigência do certificado de atributo é entre a data de emissão até o dia 31 de março do ano subsequente a emissão da CIE.

2.8 Atributos

Este campo deve conter a informação de estudante concedida ao titular do certificado de atributo com uso do tipo:

```
Attribute ::= SEQUENCE {
        type      AttributeType,
        values    SET OF AttributeValue
          -- at least one value is required
}

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType
```

São definidos como obrigatórios os seguintes componentes para o atributo estudante previsto na Lei n° 12.933/2013. O certificado de atributo emitido deve atender um dos conjuntos de OID a seguir descritos:

Conjunto 1:

a) **OID = 2.16.76.1.10.1** 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; nas 15 (quinze) posições subsequentes, o número da matrícula do estudante; nas 15 (quinze) posições subsequentes, o número do Registro Geral - RG do titular do atributo; nas 10 (dez) posições subsequentes, as siglas do órgão expedidor do RG e respectiva UF.

b**) OID = 2.16.76.1.10.2** e conteúdo = nas primeiras 40 (quarenta) posições, o nome da instituição de ensino; nas 15 (quinze) posições subsequentes, o grau de escolaridade; nas 30 (trinta) posições subsequentes, o nome do curso, nas 20 (vinte) posições subsequentes, o município da instituição e nas 2 (duas) posições subsequentes, a UF do município.

c**) OID = 2.16.76.1.4.3** e conteúdo = nome social, conforme disposto no Decreto nº 8.727, de 28 de abril de 2016.

<u>Conjunto 2 (exclusivo para CIE emitida pelo MEC:</u>

d) **OID = 2.16.76.1.10.3** 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,

e) **OID = 2.16.76.1.4.3** e conteúdo = nome social, conforme disposto no Decreto nº 8.727, de 28 de abril de 2016.

Os componentes para os atributos devem estar de acordo com as seguintes especificações:

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

b) Quando os números de CPF e RG não estiverem disponíveis, os campos correspondentes devem ser integralmente preenchidos com caracteres "zero";

c) Se o número do RG não estiver disponível, não se deve preencher o campo de órgão emissor e UF;

d) Todas informações de tamanho variável referentes a números, tais como RG, matrícula devem ser preenchidas com caracteres "zero" a sua esquerda para que seja completado o tamanho máximo disponível para o campo;

e) As 10 (dez) posições das informações sobre órgão emissor do RG e UF referem-se ao tamanho máximo, devendo ser utilizadas apenas as posições necessárias ao seu armazenamento, da esquerda para a direita. O mesmo se aplica às 22 (vinte e duas) posições das informações sobre município e UF da instituição de ensino;

f) Apenas os caracteres de A a Z, de 0 a 9, observado o disposto no item 2.4 deste documento, poderão ser utilizados, não sendo permitidos os demais caracteres especiais.

g) Quando o tamanho do campo de cada elemento do conteúdo não for suficiente para o preenchimento completo da informação correspondente, deve-se promover a truncagem ou abreviatura dessa informação.

2.9 Extensões

Este campo deve conter as informações adicionais de associação entre os titulares dos Certificados de Atributo e seus atributos. As extensões definidas pela RFC 5755 são:

- Audit Identity
- AC Targeting
- Authority Key Identifier

- Authority Information Access
- CRL Distribution Points
- No Revocation Available

São obrigatórias as seguintes extensões:

a) ***"Authority Key Identifier",* não crítica**: o campo keyIdentifier deve conter o *hash* SHA-1 da chave pública do certificado digital da EEA;
b) ***"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 recuperação da cadeia de certificação.

2.9.1 Perfil da Lista de Certificados de Atributos Revogados (LCAR)

A LCAR é recomendada no caso de carteira em formato de cartão que requer consulta a base de certificados de atributos emitidos.

2.9.1.1 Número(s) de versão

As LCARs geradas pela EEA responsável deverão implementar a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

2.9.1.2 Extensões de LCAR para certificados de atributo e de suas entradas

São obrigatórias as seguintes extensões de LCAR:

a) "***Authority Key Identifier***": deve conter o *hash* SHA-1 da chave pública da EEA que assina a LCR; e
b) "***CRL Number*", não crítica**: deve conter um número sequencial para cada LCAR emitida pela EEA.

A frequência máxima admitida para a emissão de LCAR para os certificados de atributo é de 6 (seis) meses.

3. Padronização de QR-Code associado à CIE

O padrão de QR-Code estabelecido para uso na CIE é o padrão QR-Code 2005, cuja especificação simbológica é dada pela ISO/IEC 18004:2006.

A especificação simbológica do QR-Code deve ter formatação e conteúdo conforme o caso do suporte: cartão físico ou aplicativo digital:

a) *quando a CIE estiver em cartão (suporte físico)*, o QR-Code impresso deverá representar o endereço (URL) que proverá acesso ao banco de dados para possibilitar a obtenção do certificado de atributo associado à CIE emitida;
b) *quando a CIE for digital (baseada em aplicativo)*, o QR-Code deve representar o próprio certificado de atributo em formato ".DER".

4. Requisitos do cartão (opcional)

4.1 Formato

a) Largura: 85,6 ± 0,12 mm;
b) Altura: 53,98 ± 0,05 mm;
c) Espessura: 0,76 ± 0,08 mm;
d) Bordas arredondadas raio: 3,18 ± 0,30 mm.

4.2 Material de confecção

a) PVC (em todas as camadas)
b) PET (em todas as camadas; opcional)
c) Laminação brilhante (opcional)

As características de resistência mecânica, química, entre outros, devem estar de acordo com a norma ISO/IEC 7816.

A CIE, para atender as normas estaduais ou municipais, pode conter tarja magnética de alta coercitividade. Os dados contidos nessa tarja devem respeitar as normas estaduais em relação ao uso e serviço que a CIE se prestará. O requisito de uma tarja magnética é opcional.

4.3 Chip do cartão (opcional)

4.3.1 Com contato

Todas as especificações/arquiteturas do chip com contato devem possuir características eletromagnéticas, químicas, físicas, mecânicas, de ordenamento lógico, entre outros de acordo com as recomendações ISO/IEC 7816, 10373 e 19784.

4.3.2 Sem contato

Todas as especificações/arquiteturas do chip sem contato devem possuir características eletromagnéticas, químicas, físicas, mecânicas, de ordenamento lógico, entre outros de acordo com as recomendações ISO/IEC 14443.

4.4 Cartão MIFARE (opcional)

A Carteira de Identificação Estudantil pode ser um cartão do tipo MIFARE. Os dados contidos devem respeitar as normas estaduais e municipais em relação ao uso e serviço que a CIE se prestará, como os casos de uso combinado com concessão de passe estudantil.

5. Requisitos para validação da CIE

5.1. Banco de dados de certificados de atributos

As entidades emissoras da CIE, conforme a determina a lei, devem manter e disponibilizar ao Poder Público o rol dos nomes e números de registro dos estudantes portadores da CIE. Portanto, como definido neste regulamento, para garantia da certificação digital das CIEs emitidas, todos os certificados de atributos emitidos deverão estar disponíveis em banco de dados para validação de autenticidade no caso da CIE ser emitida em cartão físico.

Nesse banco de dados deverão ser armazenadas e disponibilizadas para consulta, quando requerida, todas as informações especificadas neste regulamento no formato de certificado de atributo.

O acesso ao banco de dados via internet deve ser via protocolo “https” com certificado SSL emitido no âmbito da ICP-Brasil para a entidade emissora de CIE.

Os dados armazenados no banco de dados são privados e serão usados exclusivamente para atestar a autenticidade de cada CIE, cabendo a entidade emissora todo o tratamento necessário para garantir a privacidade e controle de acesso às informações.

Cada entidade emissora de CIE será responsável pelo conteúdo, acesso e manutenção das informações constantes no banco de dados, bem como, por sua disponibilização ao Poder Público.

5.2. Certificação digital

O certificado de atributo deve ser assinado por certificado digital ICP-Brasil da entidade emissora. O certificado digital da entidade emissora, denominado de Entidade Emissora de Atributo (EEA) da CIE deve ser do tipo A3 ou A4 conforme padrões da ICP-Brasil. Este certificado deverá ser, ainda, utilizado para a assinatura de certificados de atributos e assinatura da Lista de Certificados de Atributos Revogados. (LCAR), quando aplicável.

A validade do certificado digital ICP-Brasil da EEA não poderá ser inferior ao prazo de expiração do certificado de atributo assinado e emitido para a vigência da CIE.

5.3. Aplicativo para validação da CIE

A verificação da autenticidade da CIE deve ser feita por meio digital, atestando-se a autoria da entidade emissora e integridade do documento, a partir da validação do certificado de atributo emitido.

As informações constantes do certificado de atributo vinculado à CIE serão validadas a partir de um aplicativo padronizado e disponibilizado pelo Ministério da Educação. O aplicativo deverá validar a cadeia de certificação digital a fim de garantir a procedência do certificado digital padrão ICP-Brasil, e a autenticidade do certificado de atributo emitido.

O aplicativo de validação disponibilizado pelo MEC deverá ser capaz de validar qualquer CIE gerada com o certificado de atributo padronizado neste regulamento, independentemente da entidade emissora, desde que sejam atendidos o presente regulamento, os regulamentos e a padronização nacional da CIE, definidos pelo MEC, e as disposições da Lei nº 12.933/13.

O aplicativo de validação fornecido e padronizado pelo MEC e ITI, será o validador digital da CIE para fins de validação oficial dos requisitos nesta portaria.

5.4. Repositório de chaves públicas

Toda entidade emissora de CIE deverá cadastrar a Chave Pública do certificado ICP-Brasil utilizado para a emissão dos respectivos certificados de atributos, em repositório específico de chaves públicas, mantido pelo MEC.

A atualização do repositório de chaves públicas é de responsabilidade das entidades emissoras e é condição essencial para validação, pelo aplicativo de validação oficial fornecido pelo MEC, das CIEs emitidas. As instruções para sua atualização serão disponibilizadas no Manual Operacional da CIE, no seguinte endereço eletrônico: idestudantil.mec.gov.br.

O repositório de chaves públicas será mantido pelo MEC atendendo aos requisitos de segurança, sigilo e integridade das informações, de acordo com a legislação vigente. Deverá ser fornecido canal de comunicação para esclarecimentos e suporte sobre o processo de atualização do repositório pelas entidades emissoras.