DECISÃO DE EXECUÇÃO (UE) 2021/1073 DA COMISSÃO

de 28 de junho de 2021

que estabelece as especificações técnicas e regras para a execução do regime de confiança do Certificado Digital COVID da UE estabelecido pelo Regulamento (UE) 2021/953 do Parlamento Europeu e do Conselho

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (UE) 2021/953 do Parlamento Europeu e do Conselho relativo a um regime para a emissão, verificação e aceitação de certificados interoperáveis de vacinação, teste e recuperação da COVID-19 (Certificado Digital COVID da UE), a fim de facilitar a livre circulação durante a pandemia de COVID-19 ([1]), nomeadamente o artigo 9.º, n.os 1 e 3,

Considerando o seguinte:

(1) O Regulamento (UE) 2021/953 estabelece o Certificado Digital COVID da UE, que tem como finalidade comprovar que uma pessoa recebeu uma vacina contra a COVID-19, obteve um resultado negativo no teste ou recuperou da infeção.

(2) Para que o Certificado Digital COVID da UE esteja operacional em toda a União, é necessário estabelecer especificações técnicas e regras para preencher, emitir e verificar com segurança os certificados digitais COVID, assegurar a proteção dos dados pessoais, definir a estrutura comum do identificador único do certificado e emitir um código de barras válido, seguro e interoperável. Esse regime de confiança também define as premissas para procurar assegurar a interoperabilidade com as normas internacionais e os sistemas tecnológicos e, como tal, pode servir de modelo de cooperação a nível global.

(3) A capacidade de ler e interpretar o Certificado Digital COVID da UE exige uma estrutura de dados comum e um acordo quanto ao significado pretendido de cada campo de dados da carga útil e aos seus possíveis valores. Com vista a facilitar essa interoperabilidade, é necessário definir uma estrutura de dados comum e coordenada para o regime aplicável ao Certificado Digital COVID da UE. As orientações relativas a este regime foram desenvolvidas pela rede de saúde em linha criada com base na Diretiva 2011/24/UE do Parlamento Europeu e do Conselho ([2]). Essas orientações devem ser tomadas em consideração aquando do estabelecimento das especificações técnicas que definem o formato e a gestão da confiança para o Certificado Digital COVID da UE. Importa definir uma especificação para a estrutura de dados e os mecanismos de codificação, bem como um mecanismo de codificação de transporte num formato de leitura ótica (QR), que possa ser exibido no ecrã de um dispositivo móvel ou impresso numa folha de papel.

(4) Para além das especificações técnicas relativas ao formato e à gestão da confiança do Certificado Digital COVID da UE, importa estabelecer regras gerais para efeitos de preenchimento dos certificados, que possam ser utilizadas para os valores codificados constantes do Certificado Digital COVID da UE. Os conjuntos de valores que aplicam essas regras devem ser atualizados regularmente e publicados pela Comissão, tendo como base o trabalho relevante da rede de saúde em linha.

(5) Nos termos do Regulamento (UE) 2021/953, os certificados autênticos que compõem o Certificado Digital COVID da UE devem ser identificáveis individualmente através de um identificador único do certificado, tendo em conta que é possível emitir aos cidadãos mais do que um certificado durante o período de vigência do Regulamento (UE) 2021/953. O identificador único do certificado deve consistir numa cadeia alfanumérica e os Estados-Membros deverão assegurar que não contenha quaisquer dados que o liguem a outros documentos ou identificadores, como os números de passaporte ou de bilhete de identidade, a fim de evitar que o titular possa ser identificado. A fim de assegurar que o identificador do certificado seja único, importa estabelecer especificações técnicas e regras aplicáveis à sua estrutura comum.

([1]) JO L 211 de 15.6.2021, p. 1.

([2]) Diretiva 2011/24/UE do Parlamento Europeu e do Conselho, de 9 de março de 2011, relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços (JO L 88 de 4.4.2011, p. 45).

(6) A segurança, a autenticidade, a validade e a integridade dos certificados que compõem o Certificado Digital COVID da UE e a sua conformidade com a legislação da União em matéria de proteção de dados são fundamentais para a sua aceitação em todos os Estados-Membros. O regime de confiança que estabelece as regras aplicáveis e as infraestruturas para a emissão e a verificação fiáveis e seguras dos Certificados Digitais COVID da UE permite alcançar esses objetivos. O regime de confiança deve basear-se, nomeadamente, numa infraestrutura de chave pública com uma cadeia de confiança que vai desde as autoridades de saúde dos Estados-Membros ou outras autoridades de confiança até às entidades individuais que emitem os Certificados Digitais COVID da UE. Por conseguinte, com vista a assegurar um sistema de interoperabilidade a nível da UE, a Comissão criou um sistema central — o portal do Certificado Digital COVID da UE (o «portal») — onde são guardadas as chaves públicas utilizadas para efeitos de verificação. Quando o código QR de um certificado é lido, a assinatura digital é verificada utilizando a chave pública pertinente, previamente guardada nesse portal central. As assinaturas digitais podem ser utilizadas para assegurar a integridade e a autenticidade dos dados. As infraestruturas de chave pública criam confiança ao ligarem chaves públicas a emitentes de certificados. São utilizados no portal múltiplos certificados de chave pública para garantir a autenticidade. Para assegurar um intercâmbio seguro de dados relativamente ao material das chaves públicas entre os Estados-Membros e possibilitar uma ampla interoperabilidade, é necessário estabelecer quais os certificados de chave pública que podem ser utilizados e prever de que forma devem ser gerados.

(7) A presente decisão permite a operacionalização dos requisitos do Regulamento (UE) 2021/953 de forma a minimizar o tratamento de dados pessoais, limitando-o ao necessário para assegurar o funcionamento do Certificado Digital COVID da UE, e a contribuir para uma aplicação por parte dos responsáveis finais pelo tratamento que respeite a proteção de dados desde a conceção.

(8) Em conformidade com o Regulamento (UE) 2021/953, as autoridades ou os outros organismos designados responsáveis pela emissão dos certificados são os responsáveis pelo tratamento na aceção do artigo 4.º, n.º 7, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([3]) no exercício da sua função de tratamento de dados pessoais no decurso do processo de emissão. Dependendo da forma como os Estados-Membros organizam o processo de emissão, pode haver uma ou mais autoridades ou organismos designados, por exemplo, serviços regionais de saúde. Em conformidade com o princípio da subsidiariedade, essa escolha cabe aos Estados-Membros. Por conseguinte, os Estados-Membros são quem melhor pode assegurar, quando existem múltiplas autoridades ou outros organismos designados, que as respetivas responsabilidades dessas autoridades ou organismos sejam claramente definidas, independentemente do facto de se tratar de responsáveis pelo tratamento separados ou conjuntos (incluindo serviços regionais de saúde que criem um portal do utente conjunto para a emissão dos certificados). Da mesma forma, no que toca à verificação dos certificados pelas autoridades competentes do Estado-Membro de destino ou trânsito, ou pelos operadores de serviços de transporte de passageiros transfronteiriços que sejam obrigados pela legislação nacional a aplicar determinadas medidas de saúde pública durante a pandemia de COVID-19, esses verificadores devem cumprir as suas obrigações ao abrigo das regras de proteção de dados.

(9) Não é efetuado qualquer tipo de tratamento de dados pessoais através do portal do Certificado Digital COVID da UE, uma vez que o portal contém apenas as chaves públicas das autoridades signatárias. Essas chaves estão relacionadas com as autoridades signatárias e não permitem a reidentificação direta ou indireta de uma pessoa singular a quem tenha sido emitido um certificado. Portanto, na sua função de gestora do portal, a Comissão não deve ser um responsável pelo tratamento dos dados pessoais nem um subcontratante.

(10) A Autoridade Europeia para a Proteção de Dados foi consultada em conformidade com o disposto no artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([4]) e emitiu um parecer em 22 de junho de 2021.

(11) Considerando que as especificações técnicas e as regras são necessárias para a aplicação do Regulamento (UE) 2021/953 a partir de 1 de julho de 2021, justifica-se a aplicação imediata da presente decisão.

(12) Por conseguinte, atendendo à necessidade de uma rápida aplicação do Certificado Digital COVID da UE, a presente decisão entra em vigor no dia da sua publicação,

([3]) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

([4]) Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39).

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

As especificações técnicas do Certificado Digital COVID da UE que estabelecem a estrutura de dados genérica, os mecanismos de codificação e o mecanismo de codificação de transporte num formato de leitura ótica são definidas no anexo I.

Artigo 2.º

As regras de preenchimento dos certificados referidos no artigo 3.º, n.º 1, do Regulamento (UE) 2021/953 são definidas no anexo II da presente decisão.

Artigo 3.º

Os requisitos que estabelecem a estrutura comum do identificador único do certificado são definidos no anexo III.

Artigo 4.º

As regras de governação aplicáveis aos certificados de chave pública em relação ao portal do Certificado Digital COVID da UE e que apoiam os aspetos da interoperabilidade do regime de confiança são definidas no anexo IV.

A presente decisão entra em vigor no dia da sua publicação no *Jornal Oficial da União Europeia*.

Feito em Bruxelas, em 28 de junho de 2021.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

ANEXO I

FORMATO E GESTÃO DA CONFIANÇA

Estrutura de dados genérica, mecanismos de codificação e mecanismo de codificação de transporte num formato de leitura ótica (a seguir designado por «QR»)

1. **Introdução**

As especificações técnicas definidas no presente anexo incluem uma estrutura de dados genérica e mecanismos de codificação para o Certificado Digital COVID da UE («DCC»). Especificam ainda um mecanismo de codificação de transporte num formato de leitura ótica («QR»), que pode ser exibido no ecrã de um dispositivo móvel ou impresso. Os formatos do contentor do certificado sanitário eletrónico destas especificações são genéricos, mas utilizados, neste contexto, para incluir o DCC.

2. **Terminologia**

Para efeitos do presente anexo, entende-se por «emitentes» as organizações que utilizam estas especificações para emitir certificados sanitários e por «verificadores» as organizações que aceitam certificados sanitários como prova do estado de saúde. Por «participantes», entende-se os emitentes e os verificadores. Alguns aspetos definidos no presente anexo devem ser coordenados entre os participantes, designadamente, a gestão de um espaço de nomes e a distribuição de chaves criptográficas. Presume-se que uma entidade, a seguir designada por «secretariado», executa estas tarefas.

3. **Formato do contentor do certificado sanitário eletrónico**

O formato do contentor do certificado sanitário eletrónico («HCERT») destina-se a disponibilizar um veículo uniforme e normalizado para certificados sanitários dos diferentes emitentes («emitentes»). O objetivo das presentes especificações consiste em harmonizar a forma como esses certificados sanitários são representados, codificados e assinados com vista a facilitar a interoperabilidade.

A capacidade de ler e interpretar um DCC emitido por qualquer emitente exige uma estrutura de dados comum, bem como um acordo quanto ao significado de cada campo de dados da carga útil. A fim de facilitar essa interoperabilidade, é definida uma estrutura de dados comum e coordenada através da utilização de um esquema «JSON», que constitui o enquadramento do DCC.

3.1. *Estrutura da carga útil*

A carga útil é estruturada e codificada como CBOR com uma assinatura digital COSE, geralmente conhecida como «CBOR Web Token» (CWT) e definida no RFC 8392 ([1]). A carga útil, conforme definida nas secções seguintes, é transportada num atributo («claim») hcert.

A integridade e autenticidade de origem dos dados da carga útil devem ser verificáveis pelo verificador. A fim de disponibilizar este mecanismo, o emitente deve assinar o CWT utilizando um esquema de assinatura eletrónica assimétrico conforme definido na especificação COSE (RFC 8152 ([2])).

3.2. *Atributos CWT*

3.2.1. Descrição geral da estrutura CWT

Cabeçalho protegido

— algoritmo de assinatura (alg, etiqueta 1)

— identificador de chave (kid, etiqueta 4)

Carga útil

— emitente (iss, chave de atributo 1, opcional, ISO 3166-1 alfa-2 do emitente)

— emitido em (iat, chave de atributo 6)

— prazo de expiração (exp, chave de atributo 4)

— certificado sanitário (hcert, chave de atributo -260)

— certificado Digital COVID da UE v1 (eu_DCC_v1, chave de atributo 1)

Assinatura

([1]) rfc8392 (ietf.org).
([2]) rfc8152 (ietf.org).

3.2.2. Algoritmo de assinatura

O parâmetro do algoritmo de assinatura (alg) indica o algoritmo utilizado para a criação da assinatura. Deve cumprir ou exceder as diretrizes do SOG-IS em vigor, resumidas nos parágrafos seguintes.

São definidos um algoritmo primário e um secundário. O algoritmo secundário só deve ser utilizado se o algoritmo primário não for aceitável no âmbito das regras e dos regulamentos impostos ao emitente.

A fim de garantir a segurança do sistema, todas as implementações têm de incorporar o algoritmo secundário. Por esta razão, tanto o algoritmo primário como o secundário devem ser implementados.

Os níveis definidos pelo SOG-IS para os algoritmos primário e secundário são os seguintes:

— Algoritmo primário: o algoritmo primário é o algoritmo de assinatura digital de curva elíptica (ECDSA), conforme definido na norma (ISO/IEC 14888–3:2006), secção 2.3, utilizando os parâmetros P–256, definidos no apêndice D (D.1.2.3) da norma (FIPS PUB 186–4) em combinação com o algoritmo de dispersão SHA–256, definido na função 4 da norma (ISO/IEC 10118–3:2004).

Este corresponde ao parâmetro ES256 do algoritmo COSE.

— Algoritmo secundário: o algoritmo secundário é RSASSA-PSS conforme definido no (RFC 8230 ([3])), com um módulo de 2048 bits em combinação com o algoritmo de dispersão SHA–256, definido na função 4 da norma (ISO/IEC 10118–3:2004).

Este corresponde ao parâmetro PS256 do algoritmo COSE.

3.2.3. Identificador de chave

O atributo de identificador de chave (kid) indica o certificado de signatário de documento (DSC) que contém a chave pública a utilizar pelo verificador para controlar a exatidão da assinatura digital. A governação dos certificados de chave pública, incluindo os requisitos aplicáveis aos DSC, é descrita no anexo IV.

O atributo de identificador de chave (kid) é utilizado pelos verificadores para selecionar a chave pública correta a partir de uma lista de chaves relativas ao emitente indicadas no atributo de emitente (iss). Um emitente pode utilizar várias chaves em paralelo por razões administrativas e ao efetuar substituições de chaves. O identificador de chave não constitui um campo crítico no plano da segurança. Por esta razão, pode também ser inserido num cabeçalho não protegido, se necessário. Os verificadores devem aceitar ambas as opções. Se ambas as opções estiverem presentes, deve ser utilizado o identificador de chave do cabeçalho protegido.

Devido à redução do identificador (por razões de limite de tamanho), há uma hipótese mínima, mas não nula, de que a lista geral de DSC aceites por um verificador possa conter DSC com kid duplicado. Por esta razão, um verificador deve controlar todos os DSC com esse kid.

3.2.4. Emitente

O atributo de emitente (iss) é um valor em cadeia que pode conter opcionalmente o código de país ISO 3166-1 alfa-2 da entidade que emite o certificado sanitário. Este atributo pode ser utilizado por um verificador para identificar o conjunto de DSC a utilizar para verificação. É utilizada a chave de atributo 1 para identificar este atributo.

3.2.5. Prazo de expiração:

O atributo de prazo de expiração (exp) deve conter um selo temporal no formato de número inteiro NumericDate (conforme especificado no RFC 8392 ([4]), secção 2) indicando durante quanto tempo esta assinatura concreta da carga útil é considerada válida, após o que um verificador deve considerar que o prazo da carga útil expirou e rejeitá-la. O objetivo do parâmetro de validade é impor um limite ao período de validade do certificado sanitário. É utilizada a chave de atributo 4 para identificar este atributo.

O prazo de expiração da assinatura não deve exceder o período de validade do DSC.

([3]) rfc8230 (ietf.org).
([4]) rfc8392 (ietf.org).

3.2.6. Emitido em

O atributo «Emitido Em» (iat) deve conter um selo temporal no formato de número inteiro NumericDate (conforme especificado no RFC 8392 ([5]), secção 2) indicando a hora a que o certificado sanitário foi criado.

A data do campo «Emitido Em» não deve ser anterior ao período de validade do DSC.

Os verificadores podem aplicar políticas adicionais a fim de limitar a validade do certificado sanitário com base na hora de emissão. É utilizada a chave de atributo 6 para identificar este atributo.

3.2.7. Atributo de certificado sanitário

O atributo de certificado sanitário (hcert) é um objeto JSON (RFC 7159 ([6])) que contém as informações sobre o estado de saúde. Podem existir sob o mesmo atributo vários tipos diferentes de certificados sanitários, um dos quais o DCC.

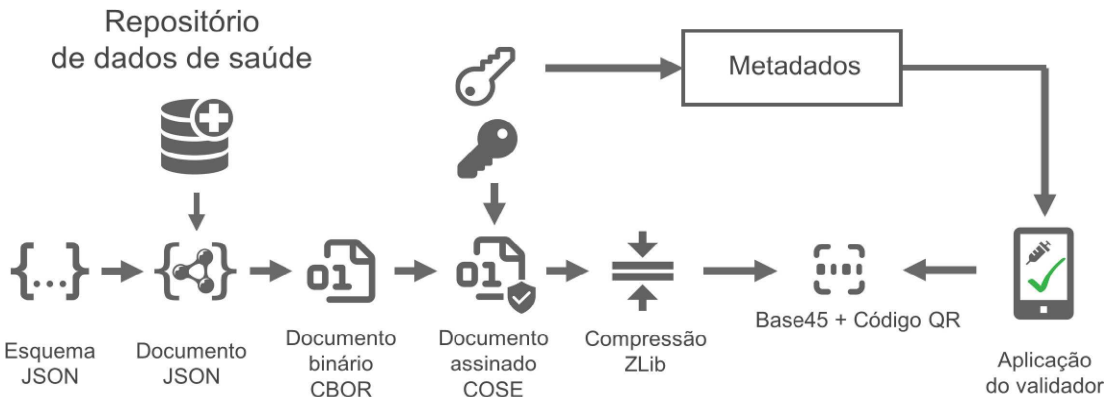
O JSON é utilizado exclusivamente para efeitos de esquema. O formato de representação é o CBOR, conforme definido no (RFC 7049 ([7])). É possível que os programadores de aplicações nunca descodifiquem ou codifiquem realmente de e para o formato JSON, mas utilizem a estrutura na memória.

A chave de atributo a utilizar para identificar este atributo é -260.

As cadeias do objeto JSON devem ser normalizadas de acordo com o Formato de Normalização de Composição Canónica (NFC) definida na norma Unicode. As aplicações de descodificação devem, todavia, ser permissivas e robustas no tocante a estes aspetos e a aceitação de qualquer conversão de tipo razoável é fortemente incentivada. Se forem detetados dados não normalizados durante a descodificação ou em funções subsequentes de comparação, as implementações devem comportar-se como se a entrada de dados fosse normalizada de acordo com o NFC.

4. **Serialização e criação da carga útil do DCC**

É aplicado o esquema seguinte como padrão de serialização:



O processo tem início com a extração de dados, por exemplo, de um repositório de dados de saúde (ou de uma fonte de dados externa) estruturando os dados extraídos de acordo com os esquemas de DCC definidos. Neste processo, a conversão para o formato de dados definido e a transformação para efeitos de legibilidade humana podem ocorrer antes de a serialização para CBOR ter início. Os acrónimos dos atributos devem ser identificados em todos os casos para os nomes visíveis antes da serialização e após a desserialização.

Não é permitida a inclusão de conteúdo de dados nacionais opcionais em certificados emitidos em conformidade com o Regulamento (UE) 2021/953 ([8]). O conteúdo de dados limita-se aos elementos de dados definidos no conjunto de dados mínimos especificado no anexo do Regulamento 2021/953.

([5]) rfc8392 (ietf.org).
([6]) rfc7159 (ietf.org).
([7]) rfc7049 (ietf.org).
([8]) Regulamento (UE) 2021/953 do Parlamento Europeu e do Conselho de 14 de junho de 2021 relativo a um regime para a emissão, verificação e aceitação de certificados interoperáveis de vacinação, teste e recuperação da COVID-19 (Certificado Digital COVID da UE), a fim de facilitar a livre circulação durante a pandemia de COVID-19, JO L 211 de 15.6.2021, p. 1.

5. **Codificações de transporte**

5.1. *Em bruto*

Para interfaces de dados arbitrárias, o contentor HCERT e as respetivas cargas úteis podem ser transferidos no estado em que se encontram, utilizando qualquer transporte de dados subjacente, fiável e seguro, de 8 bits. Estas interfaces podem incluir a comunicação de campo próximo, Bluetooth ou transferência através de um protocolo de camada de aplicação, por exemplo, a transferência de um HCERT do emitente para o dispositivo móvel de um titular.

Se a transferência do HCERT do emitente para o titular se basear numa interface apenas de apresentação (por exemplo, SMS, correio eletrónico), obviamente a codificação de transporte em bruto não se aplica.

5.2. *Código de barras*

5.2.1. Compressão da carga útil (CWT)

A fim de reduzir o tamanho e de melhorar a rapidez e a fiabilidade do processo de leitura do HCERT, o CWT deve ser comprimido utilizando o ZLIB (RFC 1950 ([9])) e o mecanismo de compressão Deflate no formato definido no RFC 1951 ([10]).

5.2.2. Código de barras QR 2D

A fim de melhor gerir equipamentos preexistentes, concebidos para funcionar com cargas úteis ASCII, o CWT comprimido é codificado como ASCII utilizando Base45 antes de ser codificado num código de barras 2D.

Deve ser utilizado o formato QR definido na norma (ISO/IEC 18004:2015) na geração do código de barras 2D. Recomenda-se uma taxa de correção de erro de «Q» (de cerca de 25 %). Uma vez que se utiliza Base45, o código QR tem de utilizar a codificação alfanumérica (modo 2, indicado pelos símbolos 0010).

Para que os verificadores possam detetar o tipo de dados codificados e selecionar o esquema de descodificação e processamento adequado, os dados codificados com Base45 (de acordo com esta especificação) devem ser precedidos da cadeia de identificadores de contexto «HC1:». As futuras versões desta especificação que tenham impacto na compatibilidade com versões anteriores devem definir um novo identificador de contexto, ao passo que o caráter a seguir a «HC» deve ser retirado do conjunto de carateres [1-9A-Z]. A ordem dos incrementos é definida segundo esta sequência, ou seja, primeiro [1-9] e depois [A-Z].

Recomenda-se que o código ótico seja representado nos meios de apresentação com uma dimensão diagonal entre 35 mm e 60 mm para suportar leitores com ótica fixa, em que os meios de apresentação devem ser colocados sobre a superfície do leitor.

Se o código ótico for impresso em papel utilizando impressoras de baixa resolução (< 300 dpi), deve ter-se cuidado para representar cada símbolo (ponto) do código QR exatamente em quadrado. A escala não proporcional terá como resultado que algumas linhas ou colunas no QR tenham símbolos retangulares, o que, em muitos casos, dificulta a legibilidade.

6. **Formato da lista de confiança (lista de CSCA e DSC)**

Cada Estado-Membro é obrigado a fornecer uma lista que inclua uma ou mais autoridades de certificação signatárias nacionais (CSCA) e uma lista de todos os certificados de signatários de documentos (DSC) válidos, bem como a manter estas listas atualizadas.

6.1. *CSCA/DSC simplificados*

A partir desta versão das especificações, os Estados-Membros não devem assumir que é utilizada qualquer informação da lista de revogação de certificados (CRL), nem que o período de utilização de chaves privadas é verificado pelos responsáveis pela implementação.

O mecanismo de validade primário será antes a presença do certificado na versão mais recente dessa lista de certificados.

([9]) rfc1950 (ietf.org).
([10]) rfc1951 (ietf.org).

6.2. *Infraestrutura de chave pública (PKI) do documento de viagem eletrónico de leitura ótica (eMRTD) da OACI e centros de confiança*

Os Estados-Membros podem utilizar uma CSCA separada, mas também podem apresentar os seus certificados CSCA de eMRTD e/ou DSC existentes, podendo mesmo optar por obtê-los junto de centros de confiança (comerciais) e apresentá-los. No entanto, qualquer DSC deve ser sempre assinado pela CSCA comunicada por esse Estado-Membro.

7. **Considerações em matéria de segurança**

Ao conceber um sistema de acordo com esta especificação, os Estados-Membros devem identificar, analisar e monitorizar determinados aspetos de segurança.

Deverão, no mínimo, ser tidos em conta os seguintes aspetos:

7.1. *Período de validade da assinatura do HCERT*

O emitente do HCERT deve limitar o período de validade da assinatura especificando um prazo de expiração da assinatura. Tal obriga o titular de um certificado sanitário a renová-lo a intervalos regulares.

O período de validade aceitável pode ser determinado por condicionalismos práticos. Por exemplo, um viajante pode não ter a possibilidade de renovar o certificado sanitário durante uma viagem ao estrangeiro. No entanto, pode também dar-se o caso de um emitente considerar que existe a possibilidade de algum tipo de comprometimento de segurança que o obrigue a retirar um DSC (invalidando todos os certificados sanitários emitidos com essa chave que ainda estejam dentro do respetivo período de validade). As consequências dessa ocorrência podem ser limitadas substituindo regularmente as chaves do emitente e exigindo a renovação de todos os certificados sanitários num intervalo razoável.

7.2. *Gestão de chaves*

A presente especificação depende largamente de mecanismos criptográficos fortes para proteger a integridade dos dados e a autenticação da origem dos dados. Por conseguinte, é fundamental manter a confidencialidade das chaves privadas.

A confidencialidade das chaves criptográficas pode ser comprometida de várias formas, nomeadamente:

— o processo de geração de chaves pode ser deficiente, resultando em chaves fracas,

— as chaves podem ser reveladas devido a erro humano,

— as chaves podem ser roubadas por criminosos externos ou internos,

— as chaves podem ser calculadas através de criptoanálise,

A fim de atenuar os riscos de o algoritmo de assinatura ser fraco, permitindo que as chaves privadas fiquem comprometidas na sequência de criptoanálise, esta especificação recomenda que todos os participantes implementem um algoritmo de assinatura secundário de recurso baseado em parâmetros diferentes ou num problema matemático diferente do primário.

Quanto aos riscos mencionados relacionados com os ambientes operacionais dos emitentes, devem ser implementadas medidas de atenuação para assegurar um controlo eficaz, nomeadamente para a geração, o armazenamento e a utilização das chaves privadas em módulos de segurança físicos (HSM). Incentiva-se fortemente a utilização de HSM para assinar certificados sanitários.

Independentemente de o emitente decidir ou não utilizar HSM, deverá ser estabelecido um calendário de substituição de chaves em que a frequência das substituições seja proporcional à exposição das chaves a redes externas, a outros sistemas e ao pessoal. Um calendário de substituição devidamente definido também limita os riscos associados a certificados sanitários emitidos erroneamente, permitindo que um emitente revogue esses certificados sanitários por lotes, retirando uma chave, se necessário.

7.3. *Validação de dados de entrada*

As presentes especificações podem ser utilizadas de uma forma que implique a receção de dados de fontes não fiáveis em sistemas que podem ser de natureza crítica. Para minimizar os riscos associados a este vetor de ataque, todos os campos de entrada devem ser devidamente validados por tipos, comprimentos e conteúdos de dados. A assinatura do emitente deverá também ser verificada antes de qualquer tratamento do conteúdo do HCERT. No entanto, a validação da assinatura do emitente implica a análise, em primeiro lugar, do cabeçalho protegido do emitente, em que um potencial atacante pode tentar injetar informações cuidadosamente elaboradas para comprometer a segurança do sistema.

8. **Gestão da confiança**

A assinatura do HCERT exige uma chave pública para verificação. Os Estados-Membros devem disponibilizar estas chaves públicas. Em última instância, cada verificador tem de dispor de uma lista de todas as chaves públicas em que está disposto a confiar (já que a chave pública não faz parte do HCERT).

O sistema consiste em (apenas) duas camadas; para cada Estado-Membro, um ou mais certificados nacionais que assinam, cada um, um ou mais certificados de signatários de documentos que são utilizados nas operações quotidianas.

Os certificados dos Estados-Membros são designados por certificados das autoridades de certificação signatárias nacionais (CSCA) e são (normalmente) autoassinados. Os Estados-Membros podem ter mais do que um (por exemplo, em caso de descentralização regional). Estes certificados CSCA assinam regularmente os certificados de signatários de documentos (DSC) utilizados para assinar HCERT.

O «secretariado» desempenha um papel funcional. Deve agregar e publicar regularmente os DSC dos Estados-Membros, depois de os ter verificado em relação à lista de certificados CSCA (que foram transmitidos e verificados por outros meios).

A lista de DSC resultante deve então apresentar o conjunto agregado de chaves públicas aceitáveis [e os identificadores de chaves (kid) correspondentes] que os verificadores podem utilizar para validar as assinaturas nos HCERT. Os verificadores devem completar e atualizar esta lista regularmente.

Essas listas específicas dos Estados-Membros podem ser adaptadas no formato adequado ao seu próprio contexto nacional. Deste modo, o formato de ficheiro desta lista de confiança pode variar; pode ser, por exemplo, um JWKS assinado (formato de conjunto de JWK de acordo com o RFC 7517 ([11]), secção 5) ou qualquer outro formato específico da tecnologia utilizada nesse Estado-Membro.

Para garantir a simplicidade, os Estados-Membros podem apresentar os seus certificados CSCA existentes a partir dos seus sistemas de eMRTD conformes com as normas da OACI ou, tal como recomendado pela OMS, criar um especificamente para este domínio de saúde.

8.1. *Identificadores de chaves (kid)*

O identificador de chave (kid) é calculado ao estabelecer a lista de chaves públicas de confiança a partir dos DSC e consiste numa impressão digital SHA-256 truncada (primeiros 8 bytes) do DSC codificada no formato DER (em bruto).

Os verificadores não precisam de calcular o identificador de chave com base no DSC e podem fazer corresponder diretamente o identificador de chave no certificado sanitário emitido ao identificador de chave na lista de confiança.

8.2. *Diferenças em relação ao modelo de confiança da PKI do eMRTD da OACI*

Embora inspirado nas melhores práticas do modelo de confiança da PKI do eMRTD da OACI, deve ser realizado um conjunto de simplificações no interesse da celeridade:

— um Estado-Membro pode apresentar vários certificados CSCA,

— o período de validade do DSC (utilização da chave) pode ser definido com qualquer duração que não exceda a do certificado CSCA e pode estar ausente,

— o DSC pode conter identificadores de políticas (utilização alargada da chave) específicos dos certificados sanitários,

— os Estados-Membros podem optar por nunca efetuar qualquer verificação das revogações publicadas, fazendo simplesmente fé nas listas de DSC que recebem diariamente do secretariado ou que coligem.

([11]) rfc7517 (ietf.org).

ANEXO II

REGRAS PARA EFEITOS DE PREENCHIMENTO DO CERTIFICADO DIGITAL COVID DA UE

As regras gerais relativas aos conjuntos de valores estabelecidos no presente anexo visam assegurar a interoperabilidade a nível semântico e devem permitir implementações técnicas uniformes no que respeita ao DCC. Os elementos constantes do presente anexo podem ser utilizados nos três contextos distintos (vacinação/teste/recuperação), conforme previsto no Regulamento (UE) 2021/953. Apenas se encontram enumerados no presente anexo os elementos que requerem normalização semântica através de conjuntos de valores codificados.

A tradução dos elementos codificados na língua nacional é da responsabilidade dos Estados-Membros.

Para todos os campos de dados não mencionados nas descrições dos conjuntos de valores seguintes, recomenda-se a codificação em UTF-8 (nome, centro de teste, emitente do certificado). Recomenda-se que os campos de dados que contêm datas de calendário (data de nascimento, data de vacinação, data da recolha de amostras para teste, data do primeiro resultado de teste positivo, datas de validade do certificado) sejam codificados de acordo com a norma ISO 8601.

Se, por alguma razão, os sistemas de codificação preferenciais enumerados abaixo não puderem ser aplicados, podem ser utilizados outros sistemas internacionais de codificação, devendo ser apresentadas recomendações sobre como fazer corresponder os códigos do outro sistema de codificação ao sistema de codificação preferencial. Pode ser utilizado texto (nomes visíveis) em casos excecionais como um mecanismo de recurso quando não estiver disponível um código adequado nos conjuntos de valores definidos.

Os Estados-Membros que utilizarem outra codificação nos seus sistemas devem fazer corresponder esses códigos aos conjuntos de valores descritos. Os Estados-Membros são responsáveis por realizar essas correspondências.

Os conjuntos de valores devem ser regularmente atualizados pela Comissão com o apoio da rede de saúde em linha e do Comité de Segurança da Saúde. Os conjuntos de valores atualizados devem ser publicados no sítio Web pertinente da Comissão, assim como na página Web da rede de saúde em linha. Deve ser fornecido um histórico de alterações.

1. **Doença ou agente visado/Doença ou agente de que o titular recuperou: COVID-19 (SARS-CoV-2 ou uma das suas variantes)**

   Sistema de codificação preferencial: SNOMED CT.

   A utilizar nos certificados 1, 2 e 3.

   Os códigos selecionados referem-se à COVID-19 ou, se forem necessárias informações mais pormenorizadas sobre a variante genética do SARS-CoV-2, a estas variantes, caso essas informações pormenorizadas sejam indispensáveis por razões epidemiológicas.

   Um exemplo de código a utilizar é o código SNOMED CT 840539006 (COVID-19).

2. **Vacina contra a COVID-19 ou profilaxia**

   Sistema de codificação preferencial: SNOMED CT ou classificação ATC.

   A utilizar no certificado 1.

   São exemplos de códigos a utilizar entre os sistemas de codificação preferenciais, os códigos SNOMED CT 1119305005 (vacina de antigénio contra o SARS-CoV-2), 1119349007 (vacina de ARN mensageiro contra o SARS-CoV-2) ou J07BX03 (vacinas contra a COVID-19). O conjunto de valores deve ser alargado quando são desenvolvidos e introduzidos novos tipos de vacinas.

3. **Vacina terapêutica contra a COVID-19**

   Sistemas de codificação preferenciais (por ordem de preferência):

   — Registo de Medicamentos da União para vacinas com autorização a nível da UE (números de autorização)

   — um registo de vacinas mundial que possa ser estabelecido pela Organização Mundial da Saúde

   — nome da vacina terapêutica noutros casos. Se o nome incluir espaços em branco, estes devem ser substituídos por um hífen (-)

Nome do conjunto de valores: vacina.

A utilizar no certificado 1.

De entre os sistemas de codificação preferenciais, um exemplo de código a utilizar é o EU/1/20/1528 (Comirnaty). Exemplo de nome de vacina a utilizar como código: Sputnik-V (que corresponde a Sputnik V).

4. **Titular da autorização de introdução no mercado ou fabricante da vacina contra a COVID-19**

Sistema de codificação preferencial:

— código da organização da EMA (sistema SPOR para ISO IDMP)

— um registo mundial de titulares da autorização de introdução no mercado ou fabricantes da vacina, que possa, nomeadamente, ser estabelecido pela Organização Mundial da Saúde

— nome da organização noutros casos. Se o nome incluir espaços em branco, estes devem ser substituídos por um hífen (-)

A utilizar no certificado 1.

De entre os sistemas de codificação preferenciais, um exemplo de código a utilizar é o ORG-100001699 (AstraZeneca AB). Exemplo de nome de organização a utilizar como código: Sinovac-Biotech (que corresponde a Sinovac Biotech).

5. **Número numa série de doses, bem como o número total de doses na série**

A utilizar no certificado 1.

Dois campos:

(1) Número de doses administradas num ciclo

(2) Número de doses previstas para um ciclo completo (específico para uma pessoa no momento da administração)

Por exemplo, 1/1, 2/2 indicará ciclo completo, incluindo a opção 1/1 no caso de vacinas que compreendam duas doses, mas em relação às quais o protocolo aplicado pelo Estado-Membro consista em administrar apenas uma dose a cidadãos que tenham sido diagnosticados com COVID-19 antes da vacinação. O número total de doses na série deve ser indicado de acordo com a informação disponível no momento em que a dose é administrada. Por exemplo, se uma vacina específica requerer uma terceira dose (reforço) à data da última injeção administrada, o segundo número de campo deve refletir esta situação (por exemplo, 2/3, 3/3, etc.).

6. **Estado-Membro ou país terceiro em que a vacina foi administrada/em que o teste foi realizado**

Sistema de codificação preferencial: códigos ISO 3166 do país.

A utilizar nos certificados 1, 2 e 3.

Conteúdo do conjunto de valores: a lista completa de códigos de 2 letras, disponível como um conjunto de valores definido em FHIR (http://hl7.org/fhir/ValueSet/iso3166-1-2).

7. **Tipo de teste**

Sistema de codificação preferencial: LOINC.

A utilizar no certificado 2 e no certificado 3, caso seja introduzido o apoio à emissão de certificados de recuperação baseados em tipos de testes diferentes do TAAN, através de um ato delegado.

Os códigos neste conjunto de valores devem referir-se ao método do teste e devem ser selecionados, pelo menos, para distinguir os testes TAAN dos testes TRDA, conforme expresso no Regulamento (UE) 2021/953.

De entre os sistemas de codificação preferenciais, um exemplo de código a utilizar é o LP217198-3 (imunoensaio rápido).

8. **Fabricante e designação comercial do teste utilizado (opcional para o teste TAAN)**

Sistema de codificação preferencial: lista do CSS de testes rápidos de antigénio, mantida pelo JRC (base de dados de dispositivos de diagnóstico *in vitro* e métodos de despistagem da COVID-19).

A utilizar no certificado 2.

O conteúdo do conjunto de valores deve incluir a seleção de um teste rápido de antigénio, conforme indicado na lista comum e atualizada de testes rápidos de antigénio à COVID-19, estabelecida com base na Recomendação do Conselho 2021/C 24/01 e aprovada pelo Comité de Segurança da Saúde. A lista é mantida pelo JRC na base de dados de dispositivos de diagnóstico *in vitro* e métodos de despistagem, em: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/ /hsc-common-recognition-rat.

Para este sistema de codificação, devem ser utilizados campos relevantes, como o identificador do dispositivo de teste, o nome do teste e do fabricante, de acordo com o formato estruturado do JRC disponível em https://covid-19-diagnostics.jrc.ec.europa.eu/devices.

9. **Resultado do teste**

Sistema de codificação preferencial: SNOMED CT.

A utilizar no certificado 2.

Os códigos selecionados devem permitir a distinção entre resultados de teste positivos e negativos (detetado ou não detetado). Podem ser adicionados mais valores (como indeterminado) se os casos de utilização o exigirem.

São exemplos de códigos a utilizar, de entre os sistemas de codificação preferenciais, o 260415000 (não detetado) e o 260373001 (detetado).

ANEXO III

ESTRUTURA COMUM DO IDENTIFICADOR ÚNICO DO CERTIFICADO

1. **Introdução**

Cada Certificado Digital COVID da UE (DCC) deve incluir um identificador único do certificado (UCI) que suporte a interoperabilidade dos DCC. O UCI pode ser utilizado para verificar o certificado. Os Estados-Membros são responsáveis pela implementação do UCI. O UCI constitui um meio de verificação da veracidade do certificado e, quando aplicável, de estabelecer a ligação a um sistema de registo (por exemplo, um IIS). Estes identificadores devem também permitir declarações (em papel e digitais) dos Estados-Membros em como as pessoas foram vacinadas ou testadas.

2. **Composição do identificador único do certificado**

O UCI deve seguir uma estrutura e um formato comuns que facilitem a interpretabilidade humana e/ou automática da informação e pode referir-se a elementos como o Estado-Membro de vacinação, a própria vacina e um identificador específico de um Estado-Membro. Garante flexibilidade aos Estados-Membros para o formatar, no pleno respeito da legislação em matéria de proteção de dados. A ordem dos diferentes elementos segue uma hierarquia definida que pode permitir futuras modificações dos blocos, sem deixar de preservar a sua integridade estrutural.

As soluções possíveis para a composição do UCI formam um espectro em que a modularidade e a interpretabilidade humana são os dois principais parâmetros de diversificação e uma característica fundamental:

— modularidade: o grau em que o código é composto de elementos constituintes distintos que contêm informações semanticamente diferentes

— interpretabilidade humana: o grau em que o código é significativo ou pode ser interpretado pelo leitor humano

— globalmente único; o identificador do país ou da autoridade é corretamente gerido; e cada país (autoridade) deve gerir corretamente o seu segmento do espaço de nomes, nunca reciclando ou reemitindo identificadores. A combinação destes fatores garante que cada identificador seja globalmente único

3. **Requisitos gerais**

Devem ser cumpridos os seguintes requisitos gerais em relação ao UCI:

(1) Conjunto de carateres: só são permitidos carateres alfanuméricos US-ASCII maiúsculos («A» a «Z», «0» a «9»); com carateres especiais adicionais para separação do RFC3986 ([1]) ([2]), designadamente {«/»,«#»,«:»};

(2) Comprimento máximo: os criadores devem ter como objetivo um comprimento de 27 a 30 carateres ([3]);

(3) Prefixo da versão: refere-se à versão do esquema do UCI. O prefixo da versão é «01» para a presente versão do documento; o prefixo da versão é composto por dois dígitos;

(4) Prefixo do país: o código do país é especificado pela norma ISO 3166-1. São reservados códigos mais longos [por exemplo, 3 carateres ou mais (por exemplo, «ACNUR»)] para utilização futura;

(5) Sufixo do código/soma de controlo:

5.1. Os Estados-Membros deverão utilizar uma soma de controlo quando for provável a ocorrência de transmissão, transcrição (humana) ou outras corrupções (ou seja, em caso de utilização de um formato impresso).

5.2. A soma de controlo não deve ser considerada para validar o certificado e não faz tecnicamente parte do identificador, mas é utilizada para verificar a integridade do código. Esta soma de controlo deverá corresponder ao resumo da norma ISO-7812-1 (LUHN-10) ([4]) de todo o UCI em formato de transporte digital/por cabo. A soma de controlo é separada do resto do UCI por um caráter «#».

([1]) rfc3986 (ietf.org).

([2]) Os campos correspondentes ao sexo, ao número do lote, ao centro de administração, à identificação do profissional de saúde ou à data da próxima vacinação podem não ser necessários para outros fins que não a utilização médica.

([3]) Para a implementação com códigos QR, os Estados-Membros podem considerar a possibilidade de utilizar um conjunto extra de carateres com um comprimento total máximo de 72 carateres (incluindo os 27-30 do próprio identificador) a fim de transmitir outras informações. Compete aos Estados-Membros definir a especificação desta informação.

([4]) O algoritmo Luhn mod N é uma extensão do algoritmo Luhn (também conhecido como algoritmo mod 10) que funciona para códigos numéricos e é usado, por exemplo, para calcular a soma de controlo dos cartões de crédito. A extensão permite que o algoritmo funcione com sequências de valores em qualquer base (neste caso, carateres alfa).

Deve ser garantida a compatibilidade com versões anteriores: os Estados-Membros que, ao longo do tempo, alterarem a estrutura dos seus identificadores (na versão principal, atualmente a v1) devem garantir que dois identificadores idênticos representem o mesmo certificado/declaração de vacinação. Por outras palavras, os Estados-Membros não podem reciclar identificadores.

4. **Opções para identificadores únicos de certificados de vacinação**

As orientações da rede de saúde em linha sobre certificados de vacinação verificáveis e elementos básicos de interoperabilidade (*eHealth Network guidelines for verifiable vaccination certificates and basic interoperability elements*) ([5]) preveem diferentes opções para os Estados-Membros e outras entidades que possam coexistir entre diferentes Estados-Membros. Os Estados-Membros podem implementar essas diferentes opções em diferentes versões do esquema do UCI.

([5]) https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf.

ANEXO IV

GOVERNAÇÃO DOS CERTIFICADOS DE CHAVE PÚBLICA

1. **Introdução**

A troca segura e fiável de chaves de assinatura para os certificados digitais COVID da UE (DCC) entre os Estados-Membros é realizada através do Portal do Certificado COVID digital da UE (DCCG), que atua como um repositório central das chaves públicas. Com o DCCG, os Estados-Membros têm a possibilidade de publicar as chaves públicas correspondentes às chaves privadas que utilizam para assinar certificados digitais COVID. Os Estados-Membros utilizadores podem recorrer ao DCCG para recolher oportunamente material atualizado sobre chaves públicas. Mais tarde, o DCCG pode ser alargado à troca de informações suplementares fiáveis fornecidas pelos Estados-Membros, como regras de validação para os DCC. O modelo de confiança do regime do DCC é uma infraestrutura de chave pública (PKI). Cada Estado-Membro mantém uma ou mais autoridades de certificação signatárias nacionais (CSCA), cujos certificados têm uma duração relativamente longa. Na sequência da decisão do Estado-Membro, a CSCA pode ser igual ou diferente da CSCA competente para os documentos de viagem de leitura ótica. A CSCA emite certificados de chave pública para os signatários de documentos nacionais de curta duração (ou seja, signatários de DCC), que são designados como certificados de signatários de documentos (DSC). A CSCA atua como uma âncora de confiança, pelo que os Estados-Membros utilizadores podem usar o certificado CSCA para validar a autenticidade e integridade dos DSC que são regularmente alterados. Uma vez efetuada a validação, os Estados-Membros podem facultar esses certificados (ou apenas as chaves públicas neles contidas) às suas aplicações de validação dos DCC. Além das CSCA e dos DSC, o DCCG também conta com a PKI para autenticar transações, assinar dados, como base de autenticação e como meio de garantir a integridade dos canais de comunicação entre os Estados-Membros e o DCCG.

As assinaturas digitais podem ser utilizadas para garantir a integridade e a autenticidade dos dados. As infraestruturas de chave pública estabelecem confiança ao associarem chaves públicas a identidades (ou emitentes) verificados. Tal é necessário para permitir que outros participantes verifiquem a origem dos dados e a identidade do parceiro de comunicação e decidam se podem confiar. No DCCG, são utilizados vários certificados de chave pública para efeitos de autenticidade. O presente anexo define os certificados de chave pública utilizados e a forma como devem ser concebidos, a fim de permitir uma ampla interoperabilidade entre os Estados-Membros. Apresenta mais informações sobre os certificados de chave pública necessários e fornece orientações sobre modelos de certificados e períodos de validade aos Estados-Membros que pretendam ter a sua própria CSCA. Uma vez que os DCC devem ser verificáveis durante um determinado período (que tem início com a emissão e expira após algum tempo), é necessário definir um modelo de verificação para todas as assinaturas aplicadas nos certificados de chave pública e nos DCC.

2. **Terminologia**

O quadro seguinte contém as abreviaturas e a terminologia utilizadas no presente anexo.

Termo	Definição
Certificado	Ou certificado de chave pública. Um certificado X.509 v3 que contém a chave pública de uma entidade
CSCA	Autoridade de certificação signatária nacional
DCC	Certificado Digital COVID da UE. Um documento digital assinado que contém informações sobre a vacinação, os testes ou a recuperação
DCCG	Portal do Certificado Digital COVID da UE. Sistema utilizado para trocar DSC entre os Estados-Membros
$DCCG_{TA}$	O certificado âncora de confiança do DCCG. A chave privada correspondente é utilizada para assinar a lista de todos os certificados CSCA fora de linha
$DCCG_{TLS}$	O certificado do servidor TLS do DCCG
DSC	Certificado de signatário de documento. O certificado de chave pública da autoridade signatária do documento de um Estado-Membro (por exemplo, um sistema autorizado a assinar DCC). Este certificado é emitido pela CSCA do Estado-Membro
EC-DSA	Algoritmo de assinatura digital de curva elíptica. Um algoritmo de assinatura criptográfica baseado em curvas elípticas
Estado-Membro	Estado-Membro da União Europeia

Termo	Definição
mTLS	TLS mútua. O protocolo de Segurança da Camada de Transporte com autenticação mútua
N.B.:	Sistema nacional de retaguarda (*backend*) de um Estado-Membro
NB_{CSCA}	O certificado CSCA de um Estado-Membro (pode ser mais do que um)
NB_{TLS}	O certificado de autenticação de cliente TLS de um sistema nacional de retaguarda
NB_{UP}	O certificado que um sistema nacional de retaguarda utiliza para assinar pacotes de dados carregados no DCCG
PKI	Infraestrutura de chave pública. Modelo de confiança baseado em certificados de chave pública e autoridades de certificação
RSA	Algoritmo criptográfico assimétrico baseado na fatorização de inteiros utilizado nas assinaturas digitais ou na cifragem assimétrica

3. **Fluxos de comunicação e serviços de segurança do DCCG**

Esta secção apresenta uma visão geral dos fluxos de comunicação e dos serviços de segurança no sistema DCCG. Define igualmente as chaves e os certificados que são utilizados para proteger a comunicação, as informações carregadas, os DCC e uma lista de confiança assinada que contém todos os certificados CSCA integrados. O DCCG funciona como uma plataforma de dados que permite o intercâmbio de pacotes de dados assinados para os Estados-Membros.

Os pacotes de dados carregados são fornecidos pelo DCCG «no estado em que se encontram», o que significa que o DCCG não adiciona nem exclui DSC dos pacotes que recebe. O sistema nacional de retaguarda (NB) dos Estados-Membros deve poder verificar a integridade e autenticidade de ponta a ponta dos dados carregados. Além disso, os sistemas nacionais de retaguarda e o DCCG utilizarão a autenticação TLS mútua para estabelecer uma ligação segura. Trata-se de um complemento às assinaturas nos dados trocados.

3.1. *Autenticação e estabelecimento da ligação*

O DCCG utiliza o protocolo de Segurança da Camada de Transporte (TLS) com autenticação mútua para estabelecer um canal cifrado autenticado entre o sistema nacional de retaguarda do Estado-Membro (NB) e o ambiente do portal. Por conseguinte, o DCCG detém um certificado de servidor TLS ($DCCG_{TLS}$) e os sistemas nacionais de retaguarda detêm um certificado de cliente TLS, (NB_{TLS}). São disponibilizados modelos de certificados na *secção 5*. Cada sistema nacional de retaguarda pode disponibilizar o seu próprio certificado TLS. Este certificado será explicitamente incluído numa lista branca e, como tal, pode ser emitido por uma autoridade de certificação de confiança pública (por exemplo, uma autoridade de certificação que cumpra os requisitos básicos do CA/Browser Forum), por uma autoridade de certificação nacional ou pode ser autoassinado. Cada Estado-Membro é responsável pelos seus dados nacionais e pela proteção da chave privada utilizada para estabelecer a ligação ao DCCG. A abordagem «traga o seu próprio certificado» requer um processo de registo e identificação bem definido, bem como procedimentos de revogação e renovação, conforme descrito nas *secções 4.1, 4.2* e *4.3*. O DCCG utiliza uma lista branca a que os certificados TLS dos N.B.: são adicionados uma vez registados com sucesso. Somente os N.B.: que se autenticam com uma chave privada correspondente a um certificado da lista branca podem estabelecer uma ligação segura ao DCCG. O DCCG também utilizará um certificado TLS que permite aos N.B.: verificar se estão efetivamente a estabelecer uma ligação ao DCCG «real» e não a alguma entidade mal-intencionada que se faz passar pelo DCCG. O certificado do DCCG será disponibilizado aos N.B.: uma vez registados com sucesso. O certificado $DCCG_{TLS}$ será emitido por uma AC de confiança pública (incluída em todos os navegadores principais). Os Estados-Membros são responsáveis por verificar se a sua ligação ao DCCG é segura (por exemplo, comparando a impressão digital do certificado $DCCG_{TLS}$ do servidor ligado com aquela que foi fornecida após o registo).

3.2. *Autoridades de certificação signatárias nacionais e modelo de validação*

Os Estados-Membros que participam no regime do DCCG devem recorrer a uma CSCA para emitir os DSC. Os Estados-Membros podem ter mais do que uma CSCA, por exemplo, em caso de descentralização regional. Cada Estado-Membro pode recorrer a autoridades de certificação existentes ou criar uma autoridade de certificação (possivelmente autoassinada) específica para o sistema DCC.

Os Estados-Membros devem apresentar o(s) seu(s) certificado(s) CSCA ao operador do DCCG durante o procedimento oficial de integração. Após a conclusão do registo do Estado-Membro (*consultar a secção 4.1 para mais informações*), o operador do DCCG atualizará uma lista de confiança assinada que contém todos os certificados CSCA que estão ativos no regime do DCC. O operador do DCCG utilizará um par de chaves assimétricas específico para assinar a lista de confiança e os certificados num ambiente fora de linha. A chave privada não será guardada no sistema DCCG em linha, de forma a evitar que um comprometimento do sistema em linha permita a um atacante comprometer a lista de confiança. O certificado âncora de confiança correspondente, DCC_{GTA}, será disponibilizado aos sistemas nacionais de retaguarda durante o processo de integração.

Os Estados-Membros podem obter a lista de confiança junto do DCCG para os seus procedimentos de verificação. A CSCA é definida como a autoridade de certificação que emite DSC; por conseguinte, os Estados-Membros que aplicam uma hierarquia de AC de vários níveis (por exemplo, AC raiz -> CSCA -> DSC) devem indicar a autoridade de certificação subordinada que emite os DSC. Neste caso, se um Estado-Membro recorrer a uma autoridade de certificação existente, o sistema DCC ignorará tudo o que esteja acima da CSCA e coloca na lista branca apenas a CSCA na qualidade de âncora de confiança (mesmo que seja uma AC subordinada). Este modelo, à semelhança do modelo da OACI, só permite exatamente 2 níveis – uma CSCA de «raiz» e um DSC de «folha» assinado apenas por essa CSCA.

Na eventualidade de um Estado-Membro explorar a sua própria CSCA, é responsável pelo funcionamento seguro e pela gestão das chaves desta AC. A CSCA atua como âncora de confiança para os DSC e, portanto, a proteção da chave privada da CSCA é essencial para a integridade do ambiente do DCC. O modelo de verificação na PKI do DCC é o modelo *shell*, segundo o qual todos os certificados na validação da cadeia de certificação devem ser válidos num determinado momento (ou seja, no momento da validação da assinatura). Por conseguinte, aplicam-se as seguintes restrições:

— a CSCA não deve emitir certificados que tenham validade superior à do próprio certificado da AC,

— o signatário do documento não deve assinar documentos que tenham validade superior à do próprio DSC,

— os Estados-Membros que exploram a sua própria CSCA devem definir períodos de validade para a sua CSCA e para todos os certificados emitidos e devem tratar da renovação dos certificados.

A *secção 4.2* inclui recomendações sobre os períodos de validade.

3.3. *Integridade e autenticidade dos dados carregados*

Os sistemas nacionais de retaguarda podem utilizar o DCCG para carregar e descarregar pacotes de dados assinados digitalmente após a conclusão da respetiva autenticação mútua. No início, estes pacotes de dados contêm os DSC dos Estados-Membros. O par de chaves utilizado pelo sistema nacional de retaguarda para a assinatura digital de pacotes de dados carregados no sistema DCCG denomina-se par de chaves de assinatura de carregamento do sistema de retaguarda nacional e o certificado de chave pública correspondente é abreviado como certificado NB_{UP}. Cada Estado-Membro traz o seu próprio certificado NB_{UP}, que pode ser autoassinado ou emitido por uma autoridade de certificação existente, como uma autoridade de certificação pública (ou seja, uma autoridade de certificação que emite o certificado de acordo com os requisitos básicos do CAB-Forum). O certificado NB_{UP} deve ser diferente de quaisquer outros certificados utilizados pelo Estado-Membro (ou seja, CSCA, cliente TLS ou DSC).

Os Estados-Membros devem fornecer o certificado de carregamento ao operador do DCCG durante o procedimento de registo inicial (*consultar a secção 4.1 para mais informações*). Cada Estado-Membro é responsável pelos seus dados nacionais e deve proteger a chave privada utilizada para assinar os carregamentos.

Outros Estados-Membros podem verificar os pacotes de dados assinados utilizando os certificados de carregamento fornecidos pelo DCCG. O DCCG verifica a autenticidade e a integridade dos dados carregados com o certificado de carregamento do N.B.: antes de serem fornecidos a outros Estados-Membros.

3.4. *Requisitos da arquitetura técnica do DCCG*

Os requisitos da arquitetura técnica do DCCG são os seguintes:

— o DCCG utiliza autenticação TLS mútua para estabelecer uma ligação cifrada autenticada aos N.B.: Deste modo, o DCCG mantém uma lista branca de certificados de cliente NB_{TLS} registados,

— o DCCG utiliza dois certificados digitais ($DCCG_{TLS}$ e $DCCG_{TA}$) com dois pares de chaves distintos. A chave privada do par de chaves $DCCG_{TA}$ é mantida fora de linha (e não nos componentes em linha do DCCG),

— o DCCG mantém uma lista de confiança dos certificados NB_{CSCA}, que é assinada com a chave privada $DCCG_{TA}$,

— as cifras utilizadas devem cumprir os requisitos da *secção 5.1*.

4. Gestão do ciclo de vida dos certificados

4.1. *Registo dos sistemas nacionais de retaguarda*

Os Estados-Membros devem registar-se junto do operador do DCCG para participarem no sistema DCCG. Esta secção descreve o procedimento técnico e operacional que deve ser seguido para registar um sistema nacional de retaguarda.

O operador do DCCG e o Estado-Membro devem trocar informações sobre as pessoas de contacto para questões técnicas relativas ao processo de integração. Presume-se que as pessoas de contacto para questões técnicas estejam habilitadas pelos respetivos Estados-Membros e a identificação/autenticação é efetuada através de outros canais. Por exemplo, a autenticação pode ser realizada quando o contacto técnico de um Estado-Membro fornece os certificados sob a forma de ficheiros cifrados por palavra-passe via correio eletrónico e partilha a palavra-passe correspondente com o operador do DCCG por telefone. Também podem ser utilizados outros canais seguros definidos pelo operador do DCCG.

O Estado-Membro deve fornecer três certificados digitais durante o processo de registo e identificação:

— o certificado TLS NB_{TLS} do Estado-Membro

— o certificado de carregamento NB_{UP} do Estado-Membro

— o(s) certificado(s) CSCA NB_{CSCA} do Estado-Membro

Todos os certificados fornecidos devem cumprir os requisitos definidos na *secção 5*. O operador do DCCG verificará se o certificado fornecido cumpre os requisitos da *secção 5*. Após a identificação e o registo, o operador do DCCG:

— adiciona o(s) certificado(s) NB_{CSCA} à lista de confiança assinada com a chave privada que corresponde à chave pública $DCCG_{TA}$,

— adiciona o certificado NB_{TLS} à lista branca do ponto final TLS do DCCG,

— adiciona o certificado NB_{UP} ao sistema DCCG,

— fornece o certificado de chave pública $DCCG_{TA}$ e $DCCG_{TLS}$ ao Estado-Membro.

4.2. *Autoridades de certificação, períodos de validade e renovação de certificados*

Caso um Estado-Membro pretenda explorar a sua própria CSCA, os certificados CSCA podem ser certificados autoassinados. Estes funcionam como âncora de confiança do Estado-Membro e, por conseguinte, o Estado-Membro deve adotar medidas sólidas para proteger a chave privada que corresponde à chave pública do certificado CSCA. Recomenda-se que os Estados-Membros utilizem um sistema fora de linha para a sua CSCA, ou seja, um sistema informático que não esteja ligado a qualquer rede. Para aceder ao sistema, deve utilizar-se um controlo por múltiplas pessoas (por exemplo, seguindo o princípio dos quatro olhos). Após a assinatura dos DSC, aplicam-se os controlos operacionais e o sistema que contém a chave privada da CSCA deve ser guardado em segurança com fortes controlos de acesso. Para proteger a chave privada da CSCA, também podem ser utilizados módulos de segurança físicos ou cartões inteligentes. Os certificados digitais têm um período de validade que obriga à renovação do certificado. A renovação é necessária para que se utilizem chaves criptográficas novas e se adaptem os tamanhos das chaves sempre que se verifiquem novos avanços informáticos ou ocorram novos ataques que ameacem a segurança do algoritmo criptográfico utilizado. Aplica-se o modelo *shell* (ver a *secção 3.2*).

Recomenda-se a aplicação dos períodos de validade seguintes, atendendo à validade de um ano dos certificados digitais COVID:

— CSCA: 4 anos

— DSC: 2 anos

— Carregamento: 1-2 anos

— Autenticação de cliente TLS: 1-2 anos

Para uma renovação em tempo útil, recomendam-se os seguintes prazos de utilização para as chaves privadas:

— CSCA: 1 ano

— DSC: 6 meses

Os Estados-Membros devem criar novos certificados de carregamento e novos certificados TLS em tempo útil, por exemplo, um mês, antes de os referidos certificados expirarem para que tudo funcione sem incidentes. Os certificados CSCA e os DSC devem ser renovados pelo menos um mês antes de terminar a utilização das chaves privadas (considerando os procedimentos operacionais necessários). Os Estados-Membros devem fornecer certificados CSCA, certificados de carregamento e certificados TLS atualizados ao operador do DCCG. Os certificados expirados devem ser retirados da lista branca e da lista de confiança.

Os Estados-Membros e o operador do DCCG devem monitorizar a validade dos seus próprios certificados. Não existe uma entidade central que mantenha um registo da validade dos certificados e informe os participantes.

4.3. *Revogação de certificados*

Em geral, os certificados digitais podem ser revogados pela AC que os emitiu utilizando listas de revogação de certificados ou o respondedor do protocolo sobre o estado do certificado em linha (OCSP). As CSCA para o sistema DCC devem fornecer listas de revogação de certificados (CRL). Mesmo que ainda não estejam a ser utilizados por outros Estados-Membros, estas CRL devem ser integradas para aplicações futuras. Caso uma CSCA decida não fornecer as CRL, os DSC dessa CSCA devem ser renovados quando as CRL passarem a ser obrigatórias. Os verificadores não devem utilizar o OCSP para validação dos DSC, mas sim as CRL. Recomenda-se que o sistema nacional de retaguarda execute a validação necessária dos DSC descarregados do Portal do DCC e que apenas remeta para os validadores nacionais dos DCC um conjunto de DSC de confiança e validados. Os validadores dos DCC não devem executar qualquer controlo da revogação dos DSC no âmbito do seu processo de validação. Uma das razões para tal prende-se com a proteção da privacidade dos titulares dos DCC evitando qualquer possibilidade de que a utilização de um DSC possa ser monitorizada pelo respondedor OCSP associado.

Os Estados-Membros podem remover os seus DSC do DCCG por sua própria iniciativa utilizando certificados de carregamento e TLS válidos. Remover um DSC significa que todos os DCC emitidos com esse DSC ficarão inválidos quando os Estados-Membros obtiverem as listas de DSC atualizadas. É fundamental proteger o material da chave privada correspondente ao DSC. Os Estados-Membros devem informar o operador do DCCG quando tiverem de revogar certificados de carregamento ou TLS, nomeadamente pelo facto de o sistema nacional de retaguarda estar comprometido. O operador do DCCG pode assim retirar a confiança depositada no certificado afetado, por exemplo, removendo-o da lista branca TLS. O operador do DCCG pode remover os certificados de carregamento da base de dados do DCCG. Os pacotes assinados com chave privada que correspondam a este certificado de carregamento ficarão inválidos quando os sistemas nacionais de retaguarda retirarem a confiança ao certificado de carregamento revogado. Caso um certificado CSCA deva ser revogado, os Estados-Membros informam o operador do DCCG, bem como os outros Estados-Membros com quem mantêm relações de confiança. O operador do DCCG emitirá uma nova lista de confiança quando o certificado afetado deixar de constar. Todos os DSC emitidos por esta CSCA ficarão inválidos quando os Estados-Membros atualizarem a loja de confiança do seu sistema nacional de retaguarda. Caso o certificado $DCCG_{TLS}$ ou o certificado $DCCG_{TA}$ deva ser revogado, o operador do DCCG e os Estados-Membros devem colaborar para criar uma nova ligação TLS de confiança e uma nova lista de confiança.

5. **Modelos de certificados**

Esta secção estabelece os requisitos e as orientações no que respeita à criptografia, bem como os requisitos relativos aos modelos dos certificados. Para os certificados DCCG, a presente secção define os modelos dos certificados.

5.1. *Requisitos de criptografia*

Os algoritmos criptográficos e as sequências de cifras TLS devem ser escolhidos com base na atual recomendação do Serviço Federal Alemão para a Segurança da Informação (BSI) ou do SOG-IS. Estas recomendações e as recomendações de outras instituições e organizações de normalização são semelhantes. É possível encontrar estas recomendações nas orientações técnicas TR 02102-1 e TR 02102-2 ([1]) ou nos Mecanismos Criptográficos Acordados (*Agreed Cryptographic Mechanisms*) do SOG-IS ([2]).

5.1.1. Requisitos aplicáveis ao DSC

Aplicam-se os requisitos previstos no *anexo I, secção 3.2.2*. Como tal, recomenda-se veementemente que os signatários dos documentos utilizem o algoritmo de assinatura digital de curva elíptica (ECDSA) com NIST-p-256 (tal como definido no apêndice D da FIPS PUB 186-4). Não são suportadas outras curvas elípticas. Devido às restrições de espaço do DCC, os Estados-Membros não devem utilizar RSA-PSS, mesmo que seja autorizado como

([1]) BSI – Orientações técnicas TR-02102 (bund.de).
([2]) SOG-IS – Documentos de apoio (sogis.eu).

algoritmo de recurso. Caso utilizem RSA-PSS, os Estados-Membros devem utilizar um módulo com 2048 ou no máximo 3072 bits de tamanho. É utilizada SHA-2 com um comprimento de saída ≥ 256 bits como função criptográfica de dispersão (ver ISO/IEC 10118-3:2004) para a assinatura do DSC.

5.1.2. Requisitos aplicáveis aos certificados TLS, de carregamento e CSCA

No caso dos certificados digitais e das assinaturas criptográficas no contexto do DCCG, os principais requisitos aplicáveis aos algoritmos criptográficos e ao comprimento das chaves encontram-se resumidos no quadro seguinte (a partir de 2021):

Algoritmo de assinatura	Tamanho da chave	Função de dispersão
EC-DSA	Mín. 250 bits	SHA-2 com um comprimento de saída ≥ 256 bits
RSA-PSS (zona de preenchimento recomendada) RSA-PKCS#1 v1.5 (zona de preenchimento pré-existente)	Mín. 3000 bits Módulo RSA (N) com um expoente público e > 2^16	SHA-2 com um comprimento de saída ≥ 256 bits
DSA	Mín. 3000 bits primo p, 250 bits chave q	SHA-2 com um comprimento de saída ≥ 256 bits

A curva elíptica recomendada para o EC-DSA é NIST-p-256 devido à sua aplicação generalizada.

5.2. *Certificado CSCA (NB_{CSCA})*

O quadro seguinte fornece orientações sobre o modelo de certificado NB_{CSCA}, caso um Estado-Membro decida explorar a sua própria CSCA para o sistema DCC.

As entradas a **negrito** são obrigatórias (e devem ser incluídas no certificado), as entradas em *itálico* são recomendadas (convém serem incluídas). Não foram definidas quaisquer recomendações para os campos em falta.

Campo	Valor
Entidade	**cn=<nome comum não vazio e único>,***o=<Fornecedor>,* **c=<Estado-Membro que explora a CSCA>**
Utilização de chave	**assinatura do certificado,***assinatura da CRL* (no mínimo)
Restrições de base	**AC = verdadeiro, restrições ao comprimento da cadeia = 0**

O nome da entidade não pode estar vazio e deve ser único dentro do Estado-Membro especificado. O código do país (c) deve corresponder ao Estado-Membro que utilizará este certificado CSCA. O certificado deve conter um identificador de chave único da entidade (SKI) de acordo com o RFC 5280 ([3]).

5.3. *Certificado de signatário de documento (DSC)*

O quadro seguinte fornece orientações sobre o DSC. As entradas a **negrito** são obrigatórias (e devem ser incluídas no certificado), as entradas em *itálico* são recomendadas (convém serem incluídas). Não foram definidas quaisquer recomendações para os campos em falta.

Campo	Valor
Número de série	**número de série único**
Entidade	**cn=<nome comum não vazio e único>**, *o=<Fornecedor>,* **c=<Estado-Membro que utiliza este DSC>**
Utilização de chave	**assinatura digital** (no mínimo)

([3]) rfc5280 (ietf.org).

O DSC deve ser assinado com a chave privada correspondente a um certificado CSCA que seja utilizado pelo Estado-Membro.

Deverão ser utilizadas as extensões seguintes:

— o certificado deve conter um identificador de chave da autoridade (AKI) que corresponda ao identificador de chave da entidade (SKI) do certificado da CSCA emitente

— o certificado deve conter um identificador de chave único da entidade (de acordo com o RFC 5280 ([4]))

Além disso, o certificado deve conter a extensão do ponto de distribuição da lista de revogação de certificados (CRL) que indica a CRL fornecida pela CSCA que emitiu o DSC.

O DSC pode conter uma extensão de utilização alargada da chave com zero ou mais identificadores de políticas de utilização de chaves que condicionam os tipos de HCERT cuja verificação este certificado permite. Se estiverem presentes um ou mais tipos, os verificadores devem verificar a utilização da chave em relação ao HCERT guardado. Para o efeito, são definidos os seguintes valores de utilização alargada da chave (extendedKeyUsage):

Campo	Valor
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.1 para os emitentes «testes»
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.2 para os emitentes «vacinação»
extendedKeyUsage	1.3.6.1.4.1.1847.2021.1.3 para os emitentes «recuperação»

Na ausência de uma extensão de utilização da chave (ou seja, sem extensões ou zero extensões), este certificado pode ser utilizado para validar qualquer tipo de HCERT. Outros documentos podem definir identificadores pertinentes adicionais da política de utilização alargada da chave utilizados com a validação de HCERT.

5.4. *Certificados de carregamento (NBUP)*

O quadro seguinte fornece orientações sobre o certificado de carregamento do sistema nacional de retaguarda. As entradas a **negrito** são obrigatórias (e devem ser incluídas no certificado), as entradas em *itálico* são recomendadas (convém serem incluídas). Não foram definidas quaisquer recomendações para os campos em falta.

Campo	Valor
Entidade	**cn=<nome comum não vazio e único>**, *o=<Fornecedor>,* **c=<Estado-Membro que utiliza este certificado de carregamento>**
Utilização de chave	**assinatura digital** (no mínimo)

5.5. *Autenticação de cliente TLS do sistema nacional de retaguarda (NB_{TLS})*

O quadro seguinte fornece orientações relativas ao certificado de autenticação de cliente TLS do sistema nacional de retaguarda. As entradas a **negrito** são obrigatórias (e devem ser incluídas no certificado), as entradas em *itálico* são recomendadas (convém serem incluídas). Não foram definidas quaisquer recomendações para os campos em falta.

Campo	Valor
Entidade	**cn=<nome comum não vazio e único>,***o=<Fornecedor>,* **c=<Estado-Membro do NB>**
Utilização de chave	**assinatura digital** (no mínimo)
Utilização alargada da chave	autenticação de cliente (1.3.6.1.5.5.7.3.2)

([4]) rfc5280 (ietf.org).

O certificado também pode conter a *autenticação do servidor (1.3.6.1.5.5.7.3.1)* com utilização alargada da chave, mas não é obrigatório.

5.6. *Certificado de assinatura da lista de confiança ($DCCG_{TA}$)*

O quadro seguinte define o certificado âncora de confiança do DCCG.

Campo	Valor
Entidade	**cn = Portal do Certificado Verde Digital** ([5])**, o=<Fornecedor>, c=<país>**
Utilização de chave	**assinatura digital** (no mínimo)

5.7. *Certificados do servidor TLS do DCCG ($DCCG_{TLS}$)*

O quadro seguinte define o certificado TLS do DCCG.

Campo	Valor
Entidade	cn=<FQDN ou endereço IP do DCCG>, o=<Fornecedor>, c=<país>
NomeAltEntidade	NomedNS: <nome DNS do DCCG> ou Endereço IP: <endereço IP do DCCG>
Utilização de chave	**assinatura digital** (no mínimo)
Utilização alargada da chave	autenticação do servidor (1.3.6.1.5.5.7.3.1)

O certificado também pode conter a *autenticação de cliente (1.3.6.1.5.5.7.3.2)* com utilização alargada da chave, mas não é obrigatório.

O certificado TLS do DCCG é emitido por uma autoridade de certificação de confiança pública (incluída em todos os navegadores e sistemas operativos principais, segundo os requisitos básicos do CA/Browser Forum).

([5]) A expressão «Certificado Verde Digital» em vez de «Certificado Digital COVID da UE» foi mantida neste contexto por ser a terminologia que foi consagrada e implementada no certificado antes de os colegisladores decidirem utilizar uma nova terminologia.