

**CINNEADH CUR CHUN FEIDHME (AE) 2021/1073 ÓN gCOIMISIÚN****an 28 Meitheamh 2021****lena leagtar síos sonraíochtaí teicniúla agus rialacha maidir le cur chun feidhme an chreata iontaoibhe i ndáil le Deimhniú Digiteach COVID AE a bunaíodh le Rialachán (AE) 2021/953 ó Pharlaimint na hEorpa agus ón gComhairle****(Téacs atá ábhartha maidir le LEE)**

TÁ AN COIMISIÚN EORPACH,

Ag féachaint don Chonradh ar Fheidhmiú an Aontais Eorpaigh,

Ag féachaint do Rialachán (AE) 2021/953 ó Pharlaimint na hEorpa agus ón gComhairle maidir le creat chun deimhnithe idir-inoibritheacha COVID-19 i ndáil le vacsaíniú, tástáil agus téarnamh (Deimhniú Digiteach COVID AE) a eisiúint agus a fhíorú, agus chun go nglacfaí leo, chun an tsaorghluaiseacht a éascú le linn phaindéim COVID-19 <sup>(1)</sup>, agus go háirithe Airteagal 9 (1) agus (3) de sin,

De bharr an mhéid seo a leanas:

- (1) Le Rialachán (AE) 2021/953 leagtar amach Deimhniú Digiteach COVID AE arb é is cuspóir dó a bheith mar chruthúnas go bhfuair duine vacsaín COVID-19, go bhfuair duine toradh diúltach ar thástáil nó gur théarnaigh duine ó ionfhabhtú.
- (2) Ionas go n-oibreoidh Deimhniú Digiteach COVID AE ar fud an Aontais, is gá sonraíochtaí teicniúla agus rialacha a bhunú chun sonraí a chur sna deimhnithe digiteacha COVID agus chun iad a eisiúint agus a fhíorú ar bhealach slán, chun cosaint sonraí pearsanta a áirithiú, struchtúr comhchoiteann aitheantóir uathúil an deimhnithe a leagan síos agus barrachód bailí, slán agus idir-inoibritheach a eisiúint. Socraíonn an creat iontaoibhe an bhuntuiscint freisin ó thaobh féachaint le hidir-inoibritheacht le caighdeán agus córais teicneolaíochta idirnáisiúnta a áirithiú, agus, mar sin, d'fhéadfadh sé an tsamhail a sholáthar maidir le comhar ar an leibhéal domhanda.
- (3) Beidh gá le struchtúr sonraí comhchoiteann agus comhaontú ar bhrí bheartaithe gach réimse sonraí i ndáil leis an bpálasta agus a luachanna féideartha ionas go mbeifí in ann Deimhniú Digiteach COVID AE a léamh agus a thuiscint. Chun idir-inoibritheacht den sórt sin a éascú, is gá struchtúr sonraí comhordaithe comhchoiteann a shainmhíniú le haghaidh an chreata de Dheimhniú Digiteach COVID AE. Rinne an Líonra ríomhShláinte a bunaíodh ar bhonn Threoir 2011/24/AE ó Pharlaimint na hEorpa agus ón gComhairle na treoirlínte a fhorbairt i ndáil leis an gcreat sin <sup>(2)</sup>. Ba cheart na treoirlínte sin a chur san áireamh agus na sonraíochtaí teicniúla a leagan síos lena leagtar amach formáid agus bainistíocht iontaoibhe i gcomhair Dheimhniú Digiteach COVID AE. Ba cheart sonraíocht maidir le struchtúr sonraí agus sásraí ionchódaithe a shonrú, chomh maith le sásra ionchódaithe iompair i bhformáid optúil atá inléite ag meaisín ("QR"), ar féidir é a léiriú ar scáileán gairis mhóibíligh nó a bheith priontáilte ar phíosa páipéir.
- (4) Chomh maith leis na sonraíochtaí teicniúla maidir le formáid agus bainistíocht iontaoibhe Dheimhniú Digiteach COVID AE, ba cheart rialacha ginearálta a bhunú chun sonraí a chur sna deimhnithe d'fhonn iad a úsáid le haghaidh luachanna códaithe i gcomhthéacs Dheimhniú Digiteach COVID AE. Ba cheart don Choimisiún na tacair luachanna lena gcuirtear na rialacha sin chun feidhme a nuashonrú agus a fhoilsiú go tráthrialta, agus leas a bhaint as obair ábhartha an Líonra ríomhShláinte.
- (5) De bhun Rialachán (AE) 2021/953, ní mór na deimhnithe barántúla a chuimseofar i nDeimhniú Digiteach COVID AE a bheith inaithianta ar leithligh trí aitheantóir uathúil an deimhnithe, ag cur san áireamh go bhféadfaí níos mó ná deimhniú amháin a eisiúint do shaoránaigh le linn na tréimhse má fhanann Rialachán (AE) 2021/953 i bhfeidhm. Beidh aitheantóir uathúil an deimhnithe comhdhéanta de theaghrán alfa-uimhriúil, agus ba cheart do na Ballstáit a áirithiú nach bhfuil aon sonraí ann a nascann le doiciméid nó le haitheantóirí eile é, sonraí amhail uimhreacha pas nó uimhreacha cárta aitheantais, ionas nach mbeifear in ann sealbhóir a shainaithint go díreach. Chun a áirithiú go bhfuil aitheantóir an deimhnithe uathúil, ba cheart sonraíochtaí teicniúla agus rialacha maidir le struchtúr comhchoiteann ina leith a leagan síos.

<sup>(1)</sup> IO L 211, 15.6.2021, lch. 1.<sup>(2)</sup> Treoir 2011/24/AE ó Pharlaimint na hEorpa agus ón gComhairle an 9 Márta 2011 maidir le cearta othar i gcúram sláinte trasteorann a chur i bhfeidhm (IO L 88, 4.4.2011, lch. 45).

- (6) Tá slándáil, barántúlacht, bailíocht agus sláine na ndeimhnithe a chuimsítear i nDeimhniú Digiteach COVID AE agus a gcomhlíontacht le dlí an Aontais maidir le cosaint sonraí fíorthábhachtach chun go nglacfar leo sna Ballstáit uile. Baintear amach na cuspóirí sin trí bhíthin an chreata iontaoibhe lena leagtar amach na rialacha maidir le heisiúint agus fíorú iontaoifa agus slán Dheimhnithe Digiteacha COVID AE, mar aon leis an mbonneagar lena mbaineann. I measc nithe eile, ba cheart an creat iontaoibhe a bheith bunaithe ar bhonneagar eochrach poiblí ag a mbeadh slabhra iontaoibhe ó údarais sláinte na mBallstát nó ó údarais iontaoifa eile go dtí na heintitis aonair a eisióinn na Deimhnithe Digiteacha COVID AE. Dá bhrí sin, d'fhonn córas idir-inoibritheach ar fud an Aontais a áirithiú, chruthaigh an Coimisiún córas lárnach – tairseach Dheimhniú Digiteach COVID AE (an “tairseach”) – ina stóráiltear eochracha poiblí a úsáidtear le haghaidh fíorú. Nuair a scantar deimhniú an chóid QR, fíoraítear an síniú digiteach leis an eochair phoiblí ábhartha, a stóráladh sa tairseach lárnach sin roimhe seo. Is féidir sínithe digiteacha a úsáid chun sláine agus barántúlacht sonraí a áirithiú. Bunaítear iontaoibh le Bonneagair Eochrach Poiblí trí eochracha poiblí a cheangal le heisitheoirí deimhnithe. Sa tairseach, úsáidtear deimhnithe eochrach poiblí iolracha le haghaidh barántúlachta. Chun malartú sonraí slán a áirithiú d'ábhar eochrach poiblí idir na Ballstáit agus chun idir-inoibritheacht fhairsing a chumasú, is gá na deimhnithe eochrach poiblí a bhunú a fhéadfar a úsáid agus faisnéis a sholáthar faoin gcaoi ar cheart iad a ghiniúint.
- (7) Foráiltear leis an gCinneadh seo go gcuirfear ceanglais Rialachán (AE) 2021/953 i bhfeidhm ar bhealach ina n-íoslaghdaítear próiseáil sonraí pearsanta go dtí an méid a bhfuil gá leis chun Deimhniú Digiteach COVID AE a chur i bhfeidhm agus a rannchuidíonn le cur chun feidhme ag rialaitheoirí deiridh ar bhealach lena n-urramaítear cosaint sonraí trí dheardh.
- (8) I gcomhréir le Rialachán (AE) 2021/953, tá na húdarais nó na comhlachtaí ainmnithe eile atá freagrach as na deimhnithe a eisiúint ina rialaitheoirí dá dtagraítear in Airteagal 4(7) de Rialachán (AE) 2016/679 ó Pharlaimint na hEorpa agus ón gComhairle <sup>(3)</sup> ina ról chun sonraí pearsanta a phróiseáil le linn an phróisis eisiúna. Ag brath ar an gcaoi a n-eagraíonn Ballstáit an próiseas eisiúna, féadfaidh údarás nó comhlacht ainmnithe amháin nó níos mó a bheith i gceist, mar shampla seirbhísí sláinte réigiúnacha. I gcomhréir le prionsabal na coimhdeachta, is de rogha an Bhallstáit é sin. Dá bhrí sin, is iad na Ballstáit féin is fearr is féidir a áirithiú, i gcás ina bhfuil roinnt údarás nó comhlachtaí ainmnithe eile i gceist, go ndéantar a bhfreagrachtaí faoi seach a leithdháileadh go soiléir, neamhspleách ar iad a bheith ina rialaitheoirí ar leithligh nó ina gcomhrialaitheoirí (lena n-áirítear seirbhísí sláinte réigiúnacha a bhunaíonn tairseach othar comhchoiteann chun na deimhnithe a eisiúint). Ar an gcaoi chéanna, maidir le fíorú deimhnithe a bheith á dhéanamh ag údarais inniúla an Bhallstáit cinn scríbe nó idirthurais, nó ag oibreoirí na seirbhísí iompair paisinéirí trasteorann a gceanglaítear orthu de réir an dlí náisiúnta bearta sláinte poiblí áirithe a chur chun feidhme le linn phaindéim COVID-19, ní mór do na fíoraitheoirí sin a gcuid oibleagáidí a chomhlíonadh faoi na rialacha maidir le cosaint sonraí.
- (9) Ní dhéantar aon sonraí pearsanta a phróiseáil trí thairseach Dheimhniú Digiteach COVID AE, mar níl sa tairseach ach eochracha poiblí na n-údarais sínithe. Baineann na heochracha sin leis na húdarais sínithe agus ní cheadaítear leo ath-shainithint dhíreach ná neamhdhíreach duine nádúrtha ar eisiúdh deimhniú dó. Ina ról mar bhainisteoir na tairsí, níor cheart don Choimisiún a bheith ina rialaitheoir ná ina phróiseálaí ar shonraí pearsanta.
- (10) Chuathas i gcomhairle leis an Maoirseoir Eorpach ar Chosaint Sonraí i gcomhréir le hAirteagal 42(1) de Rialachán (AE) 2018/1725 ó Pharlaimint na hEorpa agus ón gComhairle <sup>(4)</sup> agus thug sé tuairim uaidh an 22 Meitheamh 2021.
- (11) Ag glacadh leis go bhfuil gá le sonraíochtaí teicniúla agus rialacha chun Rialachán (AE) 2021/953 a chur i bhfeidhm ón 1 Iúil 2021, tá údar le cur i bhfeidhm láithreach an Chinnidh seo.
- (12) Dá bhrí sin, i bhfianaise an ghá le cur chun feidhme tapa Dheimhniú Digiteach COVID AE, ba cheart don Chinneadh seo teacht i bhfeidhm ar lá a fhoilsithe,

(3) Rialachán (AE) 2016/679 ó Pharlaimint na hEorpa agus ón gComhairle an 27 Aibreán 2016 maidir le daoine nádúrtha a chosaint i ndáil le sonraí pearsanta a phróiseáil agus maidir le saorghluaiseacht sonraí den sórt sin, agus lena n-aisghairtear Treoir 95/46/CE (An Rialachán Ginearálta maidir le Cosaint Sonraí) (IO L 119, 4.5.2016, lch. 1).

(4) Rialachán (AE) 2018/1725 ó Pharlaimint na hEorpa agus ón gComhairle an 23 Deireadh Fómhair 2018 maidir le daoine nádúrtha a chosaint i ndáil le sonraí pearsanta a phróiseáil ag institiúidí, comhlachtaí, oifigí agus gníomhaireachtaí an Aontais agus maidir le saorghluaiseacht na sonraí den sórt sin, agus lena n-aisghairtear Rialachán (CE) Uimh. 45/2001 agus Cinneadh Uimh. 1247/2002/CE (IO L 295, 21.11.2018, lch. 39).

TAR ÉIS AN CINNEADH SEO A GHLACADH:

*Airteagal 1*

Leagtar amach in Iarscríbhinn I na sonraíochtaí teicniúla i ndáil le Deimhniú Digiteach COVID AE lena leagtar síos an struchtúr cineálach sonraí, na sásraí ionchódaithe agus an sásra ionchódaithe iompair i bhformáid optúil atá inléite ag meaisín.

*Airteagal 2*

Leagtar amach in Iarscríbhinn II a ghabhann leis an gCinneadh seo na rialacha maidir le sonraí a chur sna deimhnithe dá dtagraítear in Airteagal 3(1) de Rialachán (AE) 2021/953.

*Airteagal 3*

Leagtar amach in Iarscríbhinn III na ceanglais lena leagtar síos struchtúr comhchoiteann aitheantóir uathúil an deimhnithe.

*Airteagal 4*

Leagtar amach in Iarscríbhinn IV na rialacha rialachais is infheidhme maidir le deimhnithe eochrach poiblí i ndáil le tairseach Dheimhniú Digiteach COVID AE a thacaíonn le gnéithe idir-inoibritheachta an chreata iontaoibhe.

Tiocfaidh an Cinneadh seo i bhfeidhm lá a fhoilsithe in *Iris Oifigiúil an Aontais Eorpaigh*.

Arna dhéanamh sa Bhruiséil, 28 Meitheamh 2021.

*Thar ceann an Choimisiúin*  
*An tUachtarán*  
Ursula VON DER LEYEN

---

## IARSCRÍBHINN I

## FORMÁID AGUS BAINISTÍOCHT IONTAOIBHE

**Struchtúr cineálach sonraí, sásraí ionchódaithe agus sásra ionchódaithe iompair i bhformáid optúil atá inléite ag meaisín (dá ngairtear ‘QR’ anseo feasta)****1. Réamhrá**

Tá struchtúr cineálach sonraí agus sásraí ionchódaithe do Dheimhniú Digiteach COVID AE (‘DDC’) le fáil sna sonraíochtaí teicniúla a leagtar amach san Iarscríbhinn seo. Sonraítear iontu sásra ionchódaithe iompair i bhformáid optúil atá inléite ag meaisín (‘QR’) freisin, a bheidh le feiceáil ar scáileán gairis mhóibíleach nó é priontáilte amach. Tá formáidí coimeádáin deimhnithe sláinte na sonraíochtaí sin cineálach, ach úsáidtear iad sa chomhthéacs seo chun DDC a iompar.

**2. Téarmaíocht**

Chun críoch na hlarscríbhinne seo, ciallaíonn ‘eistitheoir’ eagraíochtaí a úsáideann na sonraíochtaí sin chun deimhnithe sláinte a eisiúint agus ciallaíonn ‘fíoraitheoir’ eagraíochtaí a ghlacann deimhnithe sláinte mar chruthúnas ar stádas sláinte. Ciallaíonn ‘rannpháirtithe’ eistitheoirí agus fíoraitheoirí. Ní mór roinnt gnéithe a leagtar amach san Iarscríbhinn seo a chomhordú idir na rannpháirtithe, amhail bainistíocht ainmspáis agus leithdháileadh eochracha cripteagrafacha. Glactar leis go dtugann páirtí, dá dtagraítear mar ‘Ardrúnaíocht’ anseo feasta, faoi na cúraimí sin.

**3. Formáid Coimeádáin Deimhnithe Sláinte Leictreonaigh**

Dearadh an Fhormáid Coimeádáin Deimhnithe Sláinte Leictreonaigh (‘HCERT’) chun bealach aonfhoirmeach agus caighdeánach a sholáthar le haghaidh deimhnithe sláinte óna n-eistitheoirí éagsúla (‘eistitheoirí’). Is é is cuspóir do na sonraíochtaí sin an chaoi a ndéantar na deimhnithe sláinte sin a léiriú, a ionchódú agus a shíniú a chomhchuíbhiú leis an gcuspóir idir-inoibritheacht a éascú.

Éilítear struchtúr sonraí comhchoiteann agus comhaontú ar thábhacht gach réimse sonraí an phálasta chun a bheith in ann DCC a eisiúint aon eistitheoir a léamh agus a léirmhíniú. D’fhonn idir-inoibritheacht den sórt sin a éascú, déantar struchtúr sonraí comhchoiteann comhordaithe a shíniú trí úsáid scéimre ‘JSON’ atá mar fhrámú DCC.

**3.1. Struchtúr an phálasta**

Tá an pálasta struchtúrtha agus ionchódaithe mar CBOR agus síniú digiteach COSE leis. Tugtar ‘Ceadchomhartha Gréasáin CBOR’ (CWT) air de ghnáth, agus tugtar sainmhíniú air in RFC 8392 <sup>(1)</sup>. Déantar an pálasta, mar a thugtar sainmhíniú air sna ranna seo a leanas, a iompar in éileamh hcert.

Ní mór do shláine agus barántúlacht bhunús sonraí an phálasta a bheith infhíoraithe ag an bhFíoraitheoir. D’fhonn an sásra sin a sholáthar, ní mór don eistitheoir CWT a shíniú ag úsáid scéim sínithe leictreonaigh neamhshiméadrach mar a shainítear i sonraíocht COSE (RFC 8152 <sup>(2)</sup>).

**3.2. Éilimh CWT****3.2.1. Forbhreathnú ar Struchtúr CWT**

Ceanntásc Cosanta

- Algartam Sínithe (alg, lipéad 1)
- Aitheantóir Eochrach (kid, lipéad 4)

Pálasta

- Eistitheoir (iss, eochair éilimh 1, roghnach, ISO 3166-1 alfa-2 d’eistitheoir)
- Eistithe Ag (iat, eochair éilimh 6)
- Am Éaga (exp, eochair éilimh 4)
- Deimhniú Sláinte (hcrt, eochair éilimh-260)
- Deimhniú Digiteach COVID AE leagan1 (eu\_DCC\_v1, eochair éilimh 1)

Síniú

<sup>(1)</sup> rfc8392 (ietf.org)

<sup>(2)</sup> rfc8152 (ietf.org)

### 3.2.2. Algartam Sínithe

Sonraítear i bparaiméadar an Algartaim Sínithe (alg) an t-algartam a úsáidtear chun an síniú a chruthú. Ní mór dó na treoracha SOG-IT reatha, mar a achoimrítear sna míreanna seo a leanas, a chomhlíonadh nó a shárú.

Sainítear algartam príomhúil amháin agus algartam tánaisteach amháin. Níor cheart an t-algartam tánaisteach a úsáid ach amháin mura bhfuil an t-algartam príomhúil inghlactha laistigh de na rialacha agus na rialacháin a fhorchuirtear ar an eisitheoir.

D'fhonn slándáil an chórais a áirithiú, ní mór do gach cur i bhfeidhm an t-algartam tánaisteach a ionchorprú. Ar an gcúis sin, ní mór an t-algartam príomhúil agus tánaisteach a chur chun feidhme.

Is iad seo a leanas na leibhéil SOG-IT atá socraithe le haghaidh an algartaim phríomhúil agus an algartaim thánaistigh:

- An tAlgartam Príomhúil: Is Algartam Sínithe Dhigitigh Cuair Éilipsigh (ECDSA) mar a shainítear in (ISO/IEC 14888-3:2006) roinn 2.3, ag úsáid na bparaiméadar P-256 mar a shainítear in aguisín D (D.1.2.3) de (FIPS PUB 186-4) in éineacht le haisalgartam SHA-256 mar a shainítear in (ISO/IEC 10118-3:2004) feidhm 4, é an t-algartam príomhúil.

Comhfhreagraíonn sé do pharaiméadar algartaim COSE ES256.

- An tAlgartam Tánaisteach: Is RSASSA-PSS mar a shainítear in (RFC 8230 <sup>(3)</sup>) le modal de 2048 ngiotán in éineacht le haisalgartam SHA-256 mar a shainítear in (ISO/IEC 10118-3:2004) feidhm 4, é an t-algartam tánaisteach.

Comhfhreagraíonn sé do pharaiméadar algartaim COSE: PS256.

### 3.2.3. Aitheantóir Eochrach

Léiríonn an t-éileamh Aitheantóra Eochrach (kid) an Deimhniú Sínitheora Doiciméad (DSC) ina bhfuil an eochair phoiblí a úsáidfídh an fíoraitheoir chun cruinneas an tsínithe dhigitigh a sheiceáil. Rialú deimhnithe eochrach poiblí, lena n-áirítear ceanglais maidir le DSCanna, mar a shainítear in Iarscríbhinn IV.

Úsáideann fíoraitheoirí an t-éileamh Aitheantóra Eochrach (kid) chun an eochair phoiblí cheart a roghnú ó liosta d'eochracha a bhaineann leis an eisitheoir atá luaite in Éileamh an Eisitheora (iss). Féadfaidh eisitheoir roinnt eochracha a úsáid ag an am céanna chun críocha riaracháin agus nuair atá tar-rolladh eochrach á dhéanamh aige. Ní réimse slándáilchriticiúil é an tAitheantóir Eochrach. Ar an gcúis sin, féadfar é a chur ar cheanntásc neamhchosanta más gá. Ní mór d'fhíoraitheoirí an dá rogha a ghlacadh. Má tá an dá rogha ann, ní mór an tAitheantóir Eochrach sa cheanntásc cosanta a úsáid.

Mar gheall ar ghiorrú an aitheantóra (chun an méid a shrianadh) is beag seans, ach tá seans neamhnialasach ann, go mbeadh macasamhlacha kidanna de DSCanna sa liosta foriomlán de DSCanna a nglacann fíoraitheoir leo. Ar an gcúis sin, ní mór don fhíoraitheoir gach DSC a sheiceáil leis an kid sin.

### 3.2.4. Eisitheoir

Is éard atá san éileamh Eisitheora (iss) luach sreanga a d'fhéadfadh Cód Tíre alfa-2 ISO 3166-1 de chuid an eintitis a eisionn an deimhniú sláinte a bheith ann. Féadfaidh fíoraitheoir an t-éileamh sin a úsáid chun an tsraith DSC atá le húsáid le haghaidh fíorú a aithint. Úsáidtear Eochair Éilimh 1 chun an t-éileamh sin a aithint.

### 3.2.5. Am Éaga

Beidh stampa ama san fhormáid Dáta Uimhriúil (mar a shonraítear in RFC 8392 <sup>(4)</sup>, roinn 2) ag sonrú na tréimhse a bheidh an síniú áirithe sin thar an bPálasta bailí, agus i ndiaidh an dáta sin ní mór d'fhíoraitheoir diúltú don Phálasta mar a bheith in éag. Is é is cuspóir leis an bparaiméadar éaga teorainn le tréimhse bhailíochta an deimhnithe sláinte a fhórsáil. Úsáidtear Eochair Éilimh 4 chun an t-éileamh sin a aithint.

Níor cheart d'Am Éaga tréimhse bhailíochta DSC a shárú.

<sup>(3)</sup> rfc8230 (ietf.org)

<sup>(4)</sup> rfc8392 (ietf.org)

### 3.2.6. Eisithe Ag

Beidh stampa ama san fhormáid Dáta Uimhriúil (mar a shonraítear in RFC 8392 <sup>(5)</sup>, roinn 2) ag sonrú an ama ar cruthaíodh an deimhniú sláinte san éileamh Eisithe Ag (iat).

Níor cheart do réimse Eisithe Ag a bheith roimh thréimhse bhailíochta DSC.

Féadfaidh fíoraitheoirí beartais bhreise a chur i bhfeidhm chun bailíocht an deimhnithe sláinte a theorannú bunaithe ar am an eisiúna. Úsáidtear Eochair Éilimh 6 chun an t-éileamh sin a aithint.

### 3.2.7. Éileamh Deimhnithe Sláinte

Is oibiacht JSON (RFC 7159 <sup>(6)</sup>) a bhfuil faisnéis maidir le stádas sláinte atá sa Deimhniú Sláinte (hcrt). Féadfaidh cineálacha éagsúla deimhnithe sláinte a bheith ann faoin éileamh céanna, agus DCC ar cheann amháin díobh.

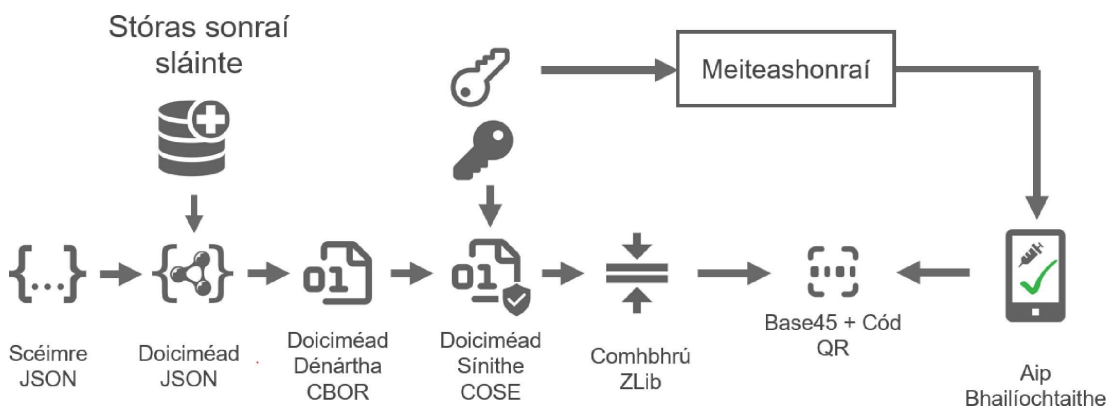
Is chun críche scéimre amháin atá JSON. Is é CBOR, mar a shainítear in (RFC 7049 <sup>(7)</sup>), an fhormáid léiriúcháin. Ní fhéadfaidh forbróirí feidhmchlár díchódú ná ionchódú ón bhformáid JSON ná chuici riamh, ach an struchtúr inchuimhne a úsáid.

Is é -260 an Eochair Éilimh atá le húsáid chun an t-éileamh sin a aithint.

Ba cheart na sreanga san oibiacht JSON a bheith NFC normalaithe de réir Comhdhéanamh Canónta Foirme Normalaithe a shainítear sa chaighdeán Unicode. Ba cheart feidhmchláir díchódaithe a bheith ceadaitheach agus láidir sna gnéithe sin, áfach, agus moltar go mór aon chineál iompaithe atá réasúnta a ghlacadh. Má thagtar ar shonraí neamhnormálaithe le linn an díchódaithe, nó i bhfeidhmeanna comparáide ina dhiaidh sin, ba cheart don fheidhm feidhmiú mar a mbeadh an t-inneachar normalaithe do NFC.

## 4. Srathú agus cruthú an phálasta DCC

Mar phatrún srathaithe, úsáidtear an scéim seo a leanas:



Tosaíonn an próiseas le baint sonraí, mar shampla, ó Stóras Sonraí Sláinte (nó ó fhoinshe sheachtrach sonraí éigin), ag struchtúru na sonraí a baineadh de réir na Scéimrí sainithe DCC. Féadfaidh iompú chuig an bhformáid sonraí sainithe agus aistriú le haghaidh inléiteacht dhaonna a tharlú sa phróiseas sin sula dtosaíonn an srathú go CBOR. Déanfar acrainmneacha na n-éileamh a mhapáil i ngach cás chun na hainmneacha roimh shrathú agus i ndiaidh díshrathú a léiriú.

Ní cheadaítear inneachar sonraí náisiúnta roghnach i ndeimhnithe a eisítear i ndiaidh Rialachán (AE) 2021/953 <sup>(8)</sup>. Tá an t-inneachar sonraí teoranta do na gnéithe sonraí atá sainithe san íostacar sonraí a shonraítear san larscríbhinn a ghabhann le Rialachán 2021/953.

<sup>(5)</sup> rfc8392 (ietf.org)

<sup>(6)</sup> rfc7159 (ietf.org)

<sup>(7)</sup> rfc7049 (ietf.org)

<sup>(8)</sup> Rialachán (AE) 2021/953 ó Pharlaimint na hEorpa agus ón gComhairle an 14 Meitheamh 2021 maidir le creat chun deimhnithe idir-inoibritheacha COVID-19 i ndáil le vacsaíní, tástáil agus téarnamh (Deimhniú Digiteach COVID AE) a eisiúint agus a fhíorú, agus chun go nglacfaí leo, chun an tsaorghluaiseacht a éascú le linn phaindéim COVID-19, IO L 211, 15.6.2021, lch. 1.

## 5. Ionchódú Iompair

### 5.1. Amh

Maidir le comhéadain sonraí treallacha, féadfar an coimeádán HCERT agus a phálastaí a aistriú mar atá, ag úsáid aon iompar sonraí bunaidh 8 ngiotán atá sábháilte agus iontaofa. Féadfaidh cumarsáid neasréimse NFC, Bluetooth nó aistriú thar phrótacal sraithe feidhmchláir, mar shampla aistriú HCERT ón Eisitheoir go gaireas móibíleach an tsealbhóra, a bheith san áireamh leis na comhéadain sin.

Má tá an t-aistriú HCERT ón Eisitheoir chuig an sealbhóir bunaithe ar an gcomhéadan léirithe-amháin (mar shampla, SMS, ríomhphost), ar ndóigh ní bheidh feidhm leis an ionchódú Amh iompair.

### 5.2. Barrachód

#### 5.2.1. Comhbhrú Pálasta (CWT)

D'fhonn an méid a laghdú agus luas agus iontaofacht a fheabhsú i bpróiseas léitheoireachta HCERT, comhbhrúfar CWT ag úsáid ZLIB (RFC 1950 <sup>(9)</sup>) agus an tsásra comhbhrúite Díbhóiscithe a shainítear in RFC 1951 <sup>(10)</sup>.

#### 5.2.2. Cód QR 2T

D'fhonn láimhseáil níos fearr a bheith ar threalamh oidhreachta a dearadh le feidhmiú ar phálastaí ASCII, déantar CWT a ionchódú mar ASCII ag úsáid Base45 sula ndéanfar é a ionchódú go barrachód 2T.

Beidh an fhormáid QR mar a shainítear in (ISO/IEC 18004:2015) in úsáid le haghaidh giniúint barrachód 2T. Moltar ráta ceartaithe earráide 'Q' (thart ar 25 %). Ós rud é go n-úsáidtear Base45, ní mór do chód QR ionchódú alfa-uimhriúla a úsáid (Mód 2, arna léiriú leis na siombailí 0010).

D'fhonn fíoraitheoirí a chumasú le bheith in ann an cineál sonraí ionchódaithe a bhrath agus an scéim díchódaithe agus próiseála cheart a roghnú, beidh an tsreang Aitheantóra Comhthéacs 'HC1:' roimh na sonraí ionchódaithe Base45 (de réir na sonraíochta seo). Déanfaidh leaganacha den tsonraíocht seo amach anseo a bhfuil tionchar acu ar shiarchomhoiriúnacht Aitheantóra Comhthéacs nua a shainiú, cé go dtógfar an carachtar a thagann i ndiaidh 'HC' ón tacar carachtar [1-9A-Z]. Sainítear an t-ord incrimintí le bheith san ord sin, i.e. [1-9] i dtosach agus [A-Z] ansin.

Moltar an cód optúil a léiriú ar na meáin láithrithe agus méid trasnánach idir 35 mm agus 60 mm air chun freastal ar léitheoirí ag a bhfuil optaic sheasta i gcás ina gcaithfear na meáin léirithe a chur ar dhromchla an léitheora.

Má tá an cód optúil priontáilte ar pháipéar ag úsáid printéirí ísealtaifigh (< 300 dpi), ní mór aire a thabhairt le gach siombail (spota) den Chód QR a léiriú i gcearnóg iomlán. Beadh siombailí dronuilleogacha i roinnt rónna nó colún in QR mar thoradh ar scálú neamhchomhréireach, agus chuirfeadh sé sin srian ar inléiteacht i neart cásanna.

## 6. Formáid Liosta Iontaoibhe (liosta CSCA agus DSC)

Ceanglaítear ar gach Ballstát liosta d'Údarás Deimhniúcháin na Tíre Sínithe (CSCA) amháin nó níos mó agus liosta de gach Deimhniú Sínitheora Doiciméad (DSC) bailí a sholáthar agus na liostaí sin a choinneáil cothrom le dáta.

### 6.1. CSCA/DSC Simplithe

De réir an leagain seo de na sonraíochtaí, ní ghlacfaidh Ballstáit leis go n-úsáidtear aon fhaisnéis ó Liosta Deimhnithe Aisghairme (CRL); ná go bhfuil an Tréimhse Úsáide Eochrach Príobháidí fíoraithe ag na daoine a chuireann é chun feidhme.

Ina áit sin, is é an príomhshásra bailíochta an deimhniú a bheith ar an leagan is déanaí den liosta deimhnithe sin.

<sup>(9)</sup> rfc1950 (ietf.org)

<sup>(10)</sup> rfc1951 (ietf.org)

## 6.2. ICAO eMRTD PKI agus Lárionaid Iontaoibhe

Féadfaidh na Ballstáit CSCA ar leithligh a úsáid – ach féadfaidh siad a ndeimhniú eMRTD CSCA agus/nó DSC reatha a chur isteach freisin; agus féadfaidh siad a roghnú fiú iad sin a fháil ó lárionaid iontaoibhe (trádála) – agus iad sin a chur isteach. Mar sin féin, ní mór aon DSC a bheith sínithe i gcónaí ag CSCA a chuir an Ballstát sin isteach.

## 7. Breithnithe Slándála

Le linn scéim a dhearadh ag úsáid na sonraíochta seo, déanfaidh na Ballstáit gnéithe slándála áirithe a aithint, a anailísiú agus déanfaidh siad faireachán orthu.

Ba cheart na gnéithe seo a leanas a bhreithniú ar a laghad:

### 7.1. Am bailíochta sínithe HCERT

Éilítear ar eisitheoir HCERTanna tréimhse bhailíochta an tsínithe a theorannú ag sonrú am éaga sínithe. Éilítear leis sin ar shealbhóir an deimhniú sláinte é a athnuachan ag eatraimh thréimhsiúla.

D'fhéadfaí an tréimhse bhailíochta inghlactha a shocrú le srianta praiticiúla. Mar shampla, d'fhéadfadh nach mbeadh féidearthacht ag taistealaí an deimhniú sláinte a athnuachan le linn turas ar an gcoigríche. Mar sin féin, d'fhéadfadh go mbeadh eisitheoir ag breithniú na féidearthachta a bhaineann le comhréiteach slándála de shórt éigin, rud a éilíonn ar an eisitheoir DSC a aistarraingt (ag neamhbhailiú gach deimhniú sláinte a eisíodh leis an eochair sin agus atá fós laistigh dá thréimhse bhailíochta). Féadfar na hiarmhairtí a bhaineann le cás mar sin a shrianadh trí eochracha Eisitheora a rolladh go tráthrialta agus athnuachan gach deimhniú sláinte a éileamh, laistigh d'eatramh réasúnta.

### 7.2. Bainistíocht eochracha

Tá an tsonraíocht seo ag brath go mór ar shásraí cripteagrafacha láidre chun sláinte sonraí agus fíorú bunúis sonraí a shocrú. Is riachtanach, dá bhrí sin, go gcoinnítear rúndacht na n-eochracha príobháideacha.

D'fhéadfaí rúndacht eochracha cripteagrafacha a chur i mbaol ar roinnt bealaí éagsúla, cuir i gcás:

- D'fhéadfadh an próiseas giniúna eochrach a bheith lochtach agus bheadh eochracha laga ann dá bharr.
- D'fhéadfadh na heochracha a bheith nochta mar gheall ar earráid daonna.
- D'fhéadfadh déantóirí cionta seachtracha nó inmheánacha na heochracha a ghoid.
- D'fhéadfaí na heochracha a ríomh ag úsáid crioptanailíse.

D'fhonn na rioscaí a bhaineann le halgartam sínithe a fhaightear a bheith lag a mhaolú, rud a cheadaíonn do na heochracha príobháideacha a bheith i mbaol trí chrioptanailís, moltar sa tsonraíocht seo do gach rannpháirtí algartam sínithe tánaiste tacachumais a chur chun feidhme bunaithe ar pharaiméadair éagsúla nó ar fhadhb mhatamaiticiúil atá éagsúil ón bhfadhb phríomhúil.

Maidir leis na rioscaí a luaitear a bhaineann le timpeallachtaí oibriúcháin na n-eisitheoirí, ba cheart bearta maolaithe a chur chun feidhme chun rialú éifeachtach a áirithiú, amhail na heochracha príobháideacha a ghiniúint, a stóráil agus a úsáid i Modúil Slándála Chrua-earraí (HSManna). Moltar go mór HSManna a úsáid chun deimhniú sláinte a shíniú.

Gan beann ar cibé a chinneann eisitheoir HSManna a úsáid nó gan iad a úsáid, ba cheart sceideal tar-rollta eochracha a bhunú i gcás ina bhfuil an mhinicíocht tarr-rollta eochracha comhréireach le neamhchosaint na n-eochracha ar líonraí seachtracha, córais eile agus pearsanra. Le sceideal tarr-rollta a roghnaíodh go maith, cuirtear srian leis na rioscaí a bhaineann le deimhniú sláinte a eisíodh trí bhotún freisin, ag cur ar chumas eisitheora deimhniú sláinte den sórt sin a aisghairm ina mbaisceanna, trí eochair a aistarraingt, más gá.

### 7.3. Bailíochtú sonraí ionchuir

Féadfar na sonraíochtaí seo a úsáid ar bhealach a thugann le fios nuair a fhaightear sonraí ó fhoinsí neamhiontaofa i gcórais a d'fhéadfadh go mbainfeadh cineál misin-chriticiúil leo. D'fhonn na rioscaí a bhaineann leis an veicteoir ionsaithe seo a íoslaghdú, ní mór gach réimse ionchuir a bhailíochtú i gceart de réir cineálacha, faid agus ionchuir sonraí. Déanfar an síniú eisitheora a fhíorú freisin sula ndéanfar aon phróiseáil ar ábhar HCERT. Mar sin féin, tugtar le fios le bailíochtú Shíniú an eisitheora go ndearnadh an Ceanntásc Cosanta Eisitheora a pharsáil i dtosach, ina bhféadfadh ionsaitheoir féideartha iarracht a dhéanamh faisnéis a chur isteach a rinneadh agus a dearadh go cúramach chun slándáil an chórais a chur i mbaol.



## 8. Bainistíocht Iontaoibhe

Éilítear eochair phoiblí chun síniú HCERT a fhíorú. Cuirfidh na Ballstáit na heochracha poiblí sin ar fáil. Ar deireadh, ní mór go mbeidh liosta de na heochracha poiblí uile ag gach fíoraitheoir, agus ní mór go mbeidh sé toilteanach iontaoibh a bheith aige as an liosta sin (mar níl an eochair phoiblí mar chuid de HCERT).

(Níl ach) dhá shraith sa chóras; maidir le gach Ballstát, deimhniú amháin nó níos mó ar an leibhéal tíre a síníonn gach ceann díobh Deimhniú Sínitheora Doiciméad amháin nó níos mó a úsáidtear in oibriúcháin laethúla.

Tugtar Údarás Deimhniúcháin na Tíre Sínithe (CSCAnna) ar na deimhnithe Ballstát agus is deimhnithe féin-shínithe iad (go hiondúil). Féadfaidh Ballstáit níos mó ná ceann amháin a bheith acu (mar shampla, i gcás díláraithe réigiúnaigh). Síníonn na deimhnithe CSCA sin na Deimhnithe Sínitheora Doiciméad (DSCanna) a úsáidtear chun HCERTanna a shíniú go tráthrialta.

Is ról feidhmiúil í an 'Ardrúnaíocht'. Déanfaidh sí DSC na mBallstát a chomhiomlánú agus a fhoilsiú go thráthrialta, tar éis iad a fhíorú in aghaidh an liosta deimhnithe CSCA (a cuireadh in iúl agus a fíoraíodh ar mhodh eile).

Soláthróidh an liosta DSCanna a fhaightear dá bharr sin an tacar comhiomlán d'eochracha poiblí inghlactha (agus na kidanna comhfhreagracha) ansin ar féidir leis na fíoraitheoirí a úsáid chun na sínithe thar HCERTanna a bhailíochtú. Ní mór d'fhíoraitheoirí an liosta sin a fháil agus a nuashonrú go tráthrialta.

Féadfar liostaí Ballstát-sonracha den sórt sin a oiriúnú i ndáil le formáid le haghaidh a suímh náisiúnta féin. Dá réir sin, d'fhéadfadh go mbeadh éagsúlacht i bhformáid comhaid an liosta iontaoibhe sin, mar shampla d'fhéadfadh sé a bheith i bhformáid JWKS (formáid shocráithe de réir RFC 7517 <sup>(1)</sup>), roinn 5) sínithe nó mar aon fhoráid eile atá sonrach don teicneolaíocht a úsáidtear sa Bhallstát sin.

D'fhonn simplíocht a áirithiú, féadfaidh na Ballstáit a ndeimhnithe reatha CSCA óna gcórais ICAO eMRTD a chur isteach, nó mar a mhol EDS, córas a chruthú go sonrach don réimse sláinte seo.

### 8.1. An tAitheantóir Eochrach (kidanna)

Déantar an t-aitheantóir eochrach (kid) a ríomh nuair atá liosta de na heochracha poiblí iontaofa ó DSCanna á chur le chéile agus is éard atá ann méarlorg giorraithe (na chéad 8 mbeart) SHA-256 de DSC ionchódaithe i bhformáid (amh) DER.

Ní gá d'fhíoraitheoirí kid a ríomh bunaithe ar an DSC agus is féidir leo an t-aitheantóir eochrach sa deimhniú sláinte eisithe a mheaitseáil go díreach leis an kid ar an liosta iontaoibhe.

### 8.2. Éagsúlachtaí sa tsamhail iontaoibhe ICAO eMRTD PKI

Cé go ndearnadh aithris ar dhea-cleachtas shamhail iontaoibhe ICAO eMRTD PKI, déanfar roinnt rudaí a shimpliú ar mhaithe le luas:

- Féadfaidh Ballstát deimhnithe iomadúla CSCA a chur isteach.
- Féadfar tréimhse bhailíochta DSC (úsáid eochrach) a shocrú ag fad ar bith gan CSCA a shárú agus d'fhéadfadh sé a bheith in easnamh.
- Féadfaidh aitheantóirí beartais (Úsáid Eochrach Shínte) atá sonrach de réir deimhnithe sláinte a bheith sa DSC.
- Féadfaidh na Ballstáit a roghnú gan aon fhíorú a dhéanamh ar aisghairmeacha foilsithe riamh; ach brath go hiomlán ar na liostaí DSC a fhaigheann siad ar bhonn laethúil ón Ardrúnaíocht nó a chuireann siad i dtoll a chéile iad féin.

---

<sup>(1)</sup> rfc7517 (ietf.org)

## IARSCRÍBHINN II

## RIALACHA CHUN CRÍCHE DEIMHNIÚ DIGITEACH COVID AE A LÍONADH

Is é is aidhm leis na rialacha ginearálta a bhaineann leis na tacair luacha a bunaíodh san Iarscríbhinn seo idir-inoibritheacht ar leibhéal séimeantach a áirithiú agus ceadóidh siad cur chun feidhme teicniúil aonfhoirmeach do DCC. Féadfar gnéithe atá san Iarscríbhinn seo a úsáid le haghaidh trí shuíomh éagsúla (vacsaíniú/tástáil/téarnamh), mar a fhoráiltear i Rialachán (AE) 2021/953. Ní liostaítear ach gnéithe lena mbaineann riachtanas caighdeánaithe shéimeantaigh trí thacair luacha códaithe san Iarscríbhinn seo.

Tá na Ballstáit freagrach as aistriúchán na ngnéithe códaithe chuig an teanga náisiúnta.

Maidir le gach réimse sonraí nach luaitear sna tuairiscí tacair luacha seo a leanas, moltar ionchódú UTF-8 (ainm, ionad tástála, eisitheoir deimhnithe). Moltar réimsí sonraí a bhfuil dátaí féilire iontu (dáta breithe, dáta an vacsaínithe, dáta bhailiú an tsampla tástála, dáta an chéad toraidh dhearfaigh ar thástáil NAAT, dátaí bailíochta deimhnithe) a ionchódú ag leanúint ISO 8601.

Má tharlaíonn sé, ar chúis ar bith, nach féidir na córais cód roghnaithe a liostaítear thíos a úsáid, féadfar córais cód idirnáisiúnta eile a úsáid agus ba cheart comhairle maidir le cóid a mhapáil ón gcóras cód eile chuig an gcóras cód roghnaithe a chur i bhfeidhm. Féadfar téacs (ainmneacha taispeána) a úsáid i gcásanna eisceachtúla mar shásra cúltaca nuair nach bhfuil cód oiriúnach ar fáil sna tacair luacha shainithe.

Ba cheart do na Ballstáit a úsáideann códú eile ina gcórais cóid den sórt sin a mhapáil chuig na tacair luacha a dtugtar tuairisc orthu. Tá na Ballstáit freagrach as aon mhapáil den sórt sin.

Déanfaidh an Coimisiún na tacair luacha a thabhairt cothrom le dáta go tráthrialta le tacaíocht ón Líonra ríomhShláinte agus ón gCoiste Slándála Sláinte. Déanfar na tacair luacha nuashonraithe a fhoilsiú ar shuíomh gréasáin ábhartha an Choimisiúin, chomh maith le leathanach gréasáin an Líonra ríomhShláinte. Ba cheart stair athruithe a sholáthar.

### 1. An galar nó an toibreán ar ar díriodh/An galar nó an toibreán ónar théarnaigh an sealbhóir: COVID-19 (SARS-CoV-2 nó ceann dá chuid athraitheach)

Córas Cód Roghnaithe: SNOMED CT.

Le húsáid i ndeimhnithe 1, 2 agus 3.

Tagróidh na cóid roghnaithe do COVID-19, nó, má theastaíonn faisnéis níos mionsonraithe ar an athraitheach géiniteach de SARS-CoV-2, do na hathraithe sin má tá gá le faisnéis mhionsonraithe mar sin ar son cúiseanna eipidéimeolaíocha.

Is sampla é an cód SNOMED CT 840539006 (COVID-19) de chód ar cheart a úsáid.

### 2. Vacsaín in aghaidh COVID-19 nó próifíolacsas in aghaidh COVID-19

Córas Cód Roghnaithe: SNOMED CT nó Rangú ATC.

Le húsáid i ndeimhniú 1.

Is sampla iad seo a leanas de chóid ar cheart a úsáid ó na córais cód roghnaithe: cód SNOMED CT 1119305005 (vacsaín antaigine SARS-CoV-2), 1119349007 (vacsaín teachtaire RNA SARS-CoV-2) nó J07BX03 (vacsaíní COVID-19). Ba cheart an tacar luacha a leathnú nuair a fhorbraítear cineálacha nua vacsaíní agus nuair a úsáidtear iad.

### 3. Táirge íocshláinte vacsaíne in aghaidh COVID-19

Córas Cód Roghnaithe (san ord roghnaithe):

- Clár an Aontais de tháirgí íocshláinte le haghaidh vacsaíní ag a bhfuil údarú uile-AE (uimhreacha údaráithe)
- Clár vacsaíní domhanda amhail ceann a d'fhéadfadh an Eagraíocht Dhomhanda Sláinte a bhunú
- Ainm an táirge íocshláinte vacsaíne i gcásanna eile. Má tá spásanna bána san ainm, ba cheart fleiscín (-) a chur ina n-áit.

Ainm an Tacair Luacha: Vacsaín.

Le húsáid i ndeimhniú 1.

Is sampla é AE/1/20/1528 (Comirnaty) de chód ar cheart a úsáid ó na córais cód roghnaithe. Is sampla é seo ar ainm vacsaíne ar cheart a úsáid mar chód: Sputnik-V (ag seasamh le haghaidh Sputnik V).

#### 4. **Sealbhóir an údaráithe le haghaidh margú vacsaíne in aghaidh COVID-19 nó monaróir na vacsaíne in aghaidh COVID-19**

Córas Cód Roghnaithe:

- Cód eagraíochta ó EMA (córas SPOR le haghaidh ISO IDMP)
- Clár domhanda sealbhóirí an údaráithe le haghaidh margú vacsaíne nó clár monaróirí, amhail ceann a d'fhéadfadh an Eagraíocht Dhomhanda Sláinte a bhunú
- Ainm na heagraíochta i gcásanna eile. Má tá spásanna bána san ainm, ba cheart fleiscín (-) a chur ina n-áit.

Le húsáid i ndeimhniú 1.

Is sampla é ORG-100001699 (AstraZeneca AB) de chód ar cheart a úsáid ón gcóras cód roghnaithe. Is sampla é seo ar ainm eagraíochta ar cheart a úsáid mar chód: Sinovac-Biotech (ag seasamh le haghaidh Sinovac Biotech).

#### 5. **Uimhir i sraith dáileog chomh maith le líon foriomlán na ndáileog sa tsraith**

Le húsáid i ndeimhniú 1.

Dhá réimse:

- (1) Uimhir na dáileoige a thugtar i sraith
- (2) Líon dáileog beartaithe le haghaidh sraith iomlán (sonrach le haghaidh duine tráth na tabhartha)

Mar shampla, tabharfaidh 1/1, 2/2 le fios go bhfuil an tabhairt críochnaithe; lena n-áirítear rogha 1/1 le haghaidh vacsaíní ag a bhfuil dá dháileog ann dóibh, ach gurb é prótacal an Bhallstáit dáileog amháin a thabhairt do shaoránaigh a diagnóisíodh go raibh COVID-19 orthu roimh an vacsaíniú. Ba cheart an líon iomlán dáileog sa tsraith a chur in iúl de réir na faisnéise atá ar fáil tráth a thugtar an dáileog. Mar shampla, má éilítear an tríú hinstealladh (teanndáileog) tráth an insteallta is déanaí a tugadh, léireofar an t-eolas sin sa dara huimhir réimse (mar shampla 2/3, 3/3 etc.).

#### 6. **An Ballstát nó an tríú tír inar tugadh an vacsaín/ina ndearnadh an tástáil**

Córas Cód Roghnaithe: Cóid Tíre ISO 3166.

Le húsáid i ndeimhniú 1, 2 agus 3.

Inneachar an tacair luacha: an liosta iomlán de chóid a bhfuil 2 litir iontu, atá ar fáil mar thacar luacha a shainítear in FHIR (<http://hl7.org/fhir/ValueSet/iso3166-1-2>)

#### 7. **An cineál tástála**

Córas Cód Roghnaithe: LOINC.

Le húsáid i ndeimhniú 2, agus i ndeimhniú 3 má thugtar tacaíocht le haghaidh eisiúint deimhniú teárnaimh bunaithe ar chineálacha eile tástála seachas NAAT isteach trí ghníomh tarmilgthe.

Tagróidh na cóid sa tacair luacha seo do mhodh na tástála agus roghnófar iad chun idirdhealú a dhéanamh idir tástálacha NAAT agus tástálacha RAT mar a léirítear i Rialachán (AE) 2021/953 ar a laghad.

Is sampla é LP217198-3 (imdhíonmheasúnacht thapa) de chód ar cheart a úsáid ón gcóras cód roghnaithe.

#### 8. **Monaróir agus ainm trádála na tástála a úsáideadh (roghnach i gcás thástáil NAAT)**

Córas Cód Roghnaithe: Liosta ó na Tástálacha Meara Antaiginí HSC mar a choimeádann an tAirmheán Comhpháirteach Taighde (Bunachar Sonraí Feistí Diagnóiseacha In Vitro COVID-19 agus Modhanna Tástála

Le húsáid i ndeimhniú 2.

Beidh san áireamh in inneachar an Tacair Luacha an rogha tástála mire antaiginí mar a liostaítear sa liosta comhchoiteann agus nuashonraithe de thástálacha meara antaiginí COVID-19, arna mbunú ar bhonn Mholadh 2021/C 24/01 ón gComhairle agus a d'aontaigh an Coiste Slándála Sláinte. Déanann an tAirmheán Comhpháirteach Taighde an liosta a choimeád sa Bhunachar Sonraí Feistí Diagnóiseacha In Vitro COVID-19 agus Modhanna Tástála ag: <https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat>

Maidir leis an gcóras cód sin, úsáidfear gach réimse ábhartha amhail aitheantóir na feiste, ainm agus monaróir na tástála, de réir fhormáid struchtúrtha an Airmheáin Chomhpháirtigh Taighde atá ar fáil ag <https://covid-19-diagnostics.jrc.ec.europa.eu/devices>

## 9. **Toradh na tástála**

Córas Cód Roghnaithe: SNOMED CT.

Le húsáid i ndeimhniú 2.

Ceadóidh na cóid a roghnófar idirdhealú idir torthaí tástála dearfacha agus diúltacha (braitheadh nó níor braitheadh). Féadfar luachanna breise (cuir i gcás neamhchinntithe) a chur leis má éilíonn na cásanna úsáide é.

Is sampla iad 260415000 (Níor braitheadh) agus 260373001 (Braitheadh) de chóid ar cheart a úsáid ón gcóras cód roghnaithe.

---

## IARSCRÍBHINN III

## STRUCTÚR COMHCHOITEANN AITHEANTÓIR UATHÚIL AN DEIMHNITHE

## 1. Réamhrá

Beidh aitheantóir uathúil deimhnithe (UCI) san áireamh le gach Deimhniú Digiteach COVID AE (DCC), agus tacóidh sé sin le hidir-inoibritheacht DCCanna. Féadfar UCI a úsáid chun an deimhniú a fhíorú. Beidh na Ballstáit freagrach as UCI a chur chun feidhme. Is modh le fírinneacht an deimhnithe a fhíorú agus, i gcás inarb infheidhme, lena nascadh le córas cláraithe (mar shampla, IIS) atá in UCI. Cumasóidh na haitheantóirí (agus iad ar páipéar agus digiteach) dearbhuithe ó na Ballstáit go bhfuair daoine aonair vacsaín nó gur tástáladh iad.

## 2. Comhdhéanamh an aitheantóra deimhnithe uathúil

Leanfaidh UCI struchtúr agus formáid chomhchoiteann a éascaíonn léirmhínteacht dhaonna agus/nó meaisíní na faisnéise agus d'fhéadfadh go mbainfeadh sé le gnéithe amhail an Ballstát vacsaínithe, an vacsaín féin agus aitheantóir sonrach Ballstáit. Áirithíonn sé solúbthacht ionas go mbeidh na Ballstáit in ann é a fhormáidiú, agus meas iomlán ar reachtaíocht maidir le cosaint sonraí. Leanann ord na ngnéithe ar leith ordlathas sainithe is féidir leasuithe ar na bloic sa todhchaí a éascú a fhad agus a choinnítear a shláine struchtúrach.

Déanfaidh na réitigh fhéideartha le haghaidh comhdhéanamh UCI speictream ina bhfuil an mhódúlacht agus an léirmhínteacht dhaonna ar an dá phríomhpharaiméadar éagsúlaithe agus an t-aon saintréith bhunúsach.

- Modúlacht: a mhéid atá an cód comhdhéanta de bhloic thógála ar leith ina bhfuil faisnéis atá difriúil ó thaobh na séimeantaice de
- Léirmhínteacht dhaonna: a mhéid atá brí le cód nó ar féidir le léitheoir daonna ciall a bhaint as
- Uathúil go domhanda; déantar bainistíocht mhaith ar an aitheantóir Tíre nó Údaráis; agus táthar ag súil go déanfaidh gach tír (údarás) bainistíocht mhaith ar a deighleog den ainmospás gan aitheantóirí a athchúrsáil ná a atheisiúint riamh. Áirithíonn an meascán sin go bhfuil gach aitheantóir uathúil go domhanda.

## 3. Ceanglais Ghinearálta

Ní mór na ceanglais uileghabhálacha seo a leanas a chomhlíonadh maidir le UCI:

- (1) Tacar carachtar: ní cheadaítear ach carachtair alfa-uimhriúla US-ASCII ('A' go 'Z', '0' go '9') le carachtair speisialta le haghaidh dealú ó RFC3986 <sup>(1)</sup> <sup>(2)</sup>, eadhon {'/', '#', ':'};
- (2) Fad uasta: ba cheart do dhearthóirí iarracht a dhéanamh fad de 27-30 carachtar a bhaint amach <sup>(3)</sup>;
- (3) Réimír leagain: tagraíonn sé sin do leagan an scéimre UCI. Is é '01' an réimír leagain don leagan seo den doiciméad; tá dhá dhigít sa réimír leagain;
- (4) Réimír tíre: sonraítear an réimír tíre le ISO 3166-1. Coimeádtar cóid níos faide (e.g. 3 carachtar agus níos mó, mar shampla 'UNHCR') le húsáid sa todhchaí;
- (5) Iarmhír cóid/Suim sheiceála:
  - 5.1. Ba cheart do na Ballstáit suim sheiceála a úsáid nuair is dócha go dtarlódh tarchur, tras-scríbhinn (daonna) nó truailliú eile (is é sin nuair a úsáidtear an fhormáid phriontáilte).
  - 5.2. Níor cheart a bheith ag brath ar an tsuim sheiceála amháin chun an deimhniú a bhailíochtú agus níl sí mar chuid den aitheantóir go teicniúil ach úsáidtear í chun sláine an chóid a fhíorú. Ba cheart an achoimre ISO-7812-1 (LUHN-10) <sup>(4)</sup> ar UCI iomlán i bhformáid iompair dhigiteach/sreinge a bheith mar an tsuim sheiceála. Tá an tsuim sheiceála scartha ón gcuid eile de UCI le carachtar '#'.

<sup>(1)</sup> rfc3986 (ietf.org)

<sup>(2)</sup> D'fhéadfadh nach mbeadh gá le réimsí amhail Inscne, Uimhir baise/luchtóige, Lárionad tabhartha, Aitheantas Gairmí Sláinte, An chéad dáta vacsaínithe eile, ach chun críche úsáide leighis amháin.

<sup>(3)</sup> Maidir le cóid QR a chur chun feidhme, d'fhéadfadh na Ballstáit sraith bhreise carachtar, suas le fad iomlán 72 carachtar (lena n-áirítear an t-aitheantóir 27-30 carachtar féin), a bhreithniú le cur leis d'fhonn faisnéis eile a chur in iúl. Is iad na Ballstáit atá freagrach as sainiú na faisnéise sin.

<sup>(4)</sup> Is síneadh é an t-alcartam 'Luhn mod N' d'alcartam Luhn (a dtugtar alcartam 'mod 10' air freisin) a oibríonn le haghaidh cóid uimhriúla agus úsáidtear é chun suim sheiceála cártaí creidmheasa a ríomh, mar shampla. Ceadáíonn an síneadh sin don alcartam oibriú le seichimh luachanna in aon bhonn (carachtair alfa-uimhriúla sa chás seo).

Ba cheart comhoiriúnacht droim ar ais a áirithiú: ní mór do Bhallstáit a athraíonn struchtúr a n-aitheantóirí thar am (laistigh den phríomhleagan, atá socruithe ag v1 faoi láthair) a áirithiú go léiríonn aon dá aitheantóir atá díreach mar an gcéanna an deimhniú/dearbhu vacsaínithe céanna. Nó, i bhfocail eile, ní féidir leis na Ballstáit aitheantóirí a athchúrsáil.

#### 4. Roghanna le haghaidh aitheantóirí deimhnithe uathúla i gcomhair deimhnithe vacsaínithe

Déantar foráil maidir le roghanna éagsúla atá ar fáil do na Ballstáit agus do pháirtithe eile a d'fhéadfadh a bheith ann i measc Ballstát éagsúla i <sup>(3)</sup> dtreoirlínte an Líonra ríomhShláinte maidir le deimhnithe vacsaínithe infhíoraithe agus bunghnéithe idir-inoibritheachta. Féadfaidh na Ballstáit roghanna éagsúla den sórt sin a úsáid i leaganacha difriúla de scéimre UCI.

---

<sup>(3)</sup> [https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof\\_interoperability-guidelines\\_en.pdf](https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf)

## IARSCRÍBHINN IV

## RIALÚ DEIMHNITHE EOCHRACH POIBLÍ

## 1. Réamhrá

Is trí Thairseach Dheimhniú Digiteach COVID AE (DCCG), a ghníomhaíonn mar stór lárnach do na heochracha poiblí, a dhéantar eochracha sínithe le haghaidh Deimhnithe Digiteacha COVID AE (DCCanna) a mhalartú go slán agus go hiontaofa idir na Ballstáit. Le DCCG, cumhachtaítear na Ballstáit leis na heochracha poiblí a chomhfhreagraíonn do na heochracha príobháideacha a úsáideann siad chun deimhnithe COVID a shíniú a fhoilsiú. Féadfaidh na Ballstáit atá ag brath DCCG a úsáid le hábhar cothrom le dáta a fháil ar eochracha poiblí ar bhonn tráthúil. Ina dhiaidh sin, féadfar DCCG a leathnú chun faisnéis bhreise iontaofa a sholáthraíonn na Ballstáit, amhail rialacha bailíochtúcháin le haghaidh DCCanna, a mhalartú. Is é Bonneagar Eochrach Poiblí (PKI) an tsamhail iontaoibhe de chreat DCC. Coinníonn gach Ballstáit Údarás Deimhniúcháin na Tíre Sínithe (CSCA) amháin, nó níos mó, ar bun agus baineann tréimhse sách fada le bailíocht na ndeimhnithe a eisíonn an t-údarás (na húdaráis) sin. I ndiaidh cinneadh ón mBallstát, féadfaidh CSCA a bheith mar CSCA mar a úsáideadh le haghaidh doiciméid iompair inléite ag meaisín, nó a bheith éagsúil ó CSCA mar sin. Eisíonn CSCA deimhnithe eochrach poiblí le haghaidh Sínitheoirí Doiciméad náisiúnta gearrshaolacha (i.e. sínitheoirí le haghaidh DCCanna), a dtugtar Deimhnithe Sínitheora Doiciméad (DSCanna) orthu. Gníomhaíonn CSCA mar chúltaca iontaofa ar bhealach is féidir leis na Ballstáit atá ag brath an deimhniú CSCA a úsáid chun barántúlacht agus sláine na DSCanna a athraíonn go tráthrialta a bhailíochtú. Nuair a bhailíochtaítear iad, féadfaidh na Ballstáit na deimhnithe sin (nó na heochracha poiblí atá le fáil iontu amháin) a sholáthar dá bhfeidhmeanna bailíochtaithe DCC. Seachas CSCanna agus DSCanna, bíonn DCCG ag brath freisin ar PKI le hidirbhearta a fhíordheimhniú agus sonraí a shíniú mar an bonn fíordheimhniúcháin agus mar mhodh le sláine na gcainéal cumarsáide idir na Ballstáit agus DCCG a áirithiú.

Is féidir sínithe digiteacha a úsáid chun sláine agus barántúlacht sonraí a bhaint amach. Bunaítear iontaoibh le Bonneagair Eochrach Poiblí trí eochracha poiblí a cheangal le céannachtaí (nó eisitheoirí) fíoraithe. Tá gá leis sin chun go mbeidh rannpháirtithe eile in ann bunús na sonraí agus céannacht an pháirtithe cumarsáide a fhíorú chun cinneadh a dhéanamh faoi iontaofacht. In DCCG, úsáidtear deimhnithe eochrach poiblí iolracha ar mhaithe le barántúlacht. Sainítear cibé deimhnithe eochrach poiblí a úsáidtear agus conas a dhearfai iad san Iarscríbhinn seo d'fhonn idir-inoibritheacht leathan i measc na mBallstát a cheadú. Soláthraíonn sé tuilleadh sonraí ar na deimhnithe eochrach poiblí is gá agus tugann sé treoir ar theimpléid deimhnithe agus tréimhsí bailíochta le haghaidh na mBallstát ar mian leo CSCA dá gcuid féin a fheidhmiú. Ós rud é go mbeidh DCCanna infhíoraithe le haghaidh tréimhse shainithe (ag tosú ón dáta eisiúna, agus a rachaidh in éag tar éis tréimhse áirithe a shonraítear), is gá samhail fíorúcháin a sháiniú le haghaidh gach sínithe a chuirtear i bhfeidhm ar na deimhnithe eochrach poiblí agus DCCanna.

## 2. Téarmaíocht

Tá giorrúcháin agus téarmaíocht a úsáidtear san Iarscríbhinn seo le fáil sa tábla seo a leanas.

| Aibíochta           | Sainmhíniú                                                                                                                                                                                             |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Deimhniú            | Nó deimhniú eochrach poiblí. Deimhniú X.509 v3 a bhfuil eochair phoiblí eintitis ann                                                                                                                   |
| CSCA                | Údarás Deimhniúcháin na Tíre Sínithe                                                                                                                                                                   |
| DCC                 | Deimhniú Digiteach COVID AE Doiciméad digiteach sínithe a bhfuil faisnéis vacsaínithe, tástála nó téarnaimh ann                                                                                        |
| DCCG                | Tairseach Dheimhniú Digiteach COVID AE Úsáidtear an córas sin chun DSCanna a mhalartú idir na Ballstáit                                                                                                |
| DCCG <sub>TA</sub>  | Deimhniú Chúltaca Iontaoibhe DCCG. Úsáidtear an eochair phríobháideach chomhfhreagrach chun an liosta de gach deimhniú CSCA a shíniú as líne                                                           |
| DCCG <sub>TLS</sub> | Deimhniú freastalaí TLS de chuid DCCG                                                                                                                                                                  |
| DSC                 | Deimhniú Sínitheora Doiciméad Deimhniú Eochrach Poiblí de chuid údaráis sínithe doiciméad Ballstáit (mar shampla, córas a cheadaítear le DCCanna a shíniú). Eisíonn CSCA an Bhallstáit an deimhniú sin |
| EC-DSA              | Algartam Sínithe Dhigitigh Cuair Éilipsigh Algartam sínithe cripteagrafach atá bunaithe ar chuair éilipseacha                                                                                          |
| Ballstát            | Ballstát de chuid an Aontais Eorpaigh                                                                                                                                                                  |

| Aibíochta          | Sainmhíniú                                                                                                                                                  |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mTLS               | TLS frithpháirteach. Prótacal Slándála Shraith an Iompair le fíordheimhniú frithpháirteach                                                                  |
| NB                 | Cúl náisiúnta de chuid Ballstáit                                                                                                                            |
| NB <sub>CSCA</sub> | Deimhniú CSCA de chuid Ballstáit (d'fhéadfadh ní ba mhó dá ceann amháin a bheith ann)                                                                       |
| NB <sub>TLS</sub>  | Deimhniú barántúlachta cliaint TLS de chuid cúil náisiúnta                                                                                                  |
| NB <sub>UP</sub>   | Deimhniú a úsáideann cúl náisiúnta chun pacáistí sonraí a uaslódáiltear chuig DCCG a shíniú                                                                 |
| PKI                | Bonneagar Eochrach Poiblí Samhail iontaoibhe bunaithe ar dheimhnithe eochrach poiblí agus údaráis deimhniúcháin                                             |
| RSA                | Algartam cripteagrafach neamhshiméadrach bunaithe ar fhachtóiriú slánuimhreacha a úsáidtear le haghaidh sínithe digiteacha nó criptiúcháin neamhshiméadrach |

### 3. Sreafaí cumarsáide agus seirbhísí slándála DCCG

Tugtar forbhreathnú sa roinn seo ar shreafaí cumarsáide agus seirbhísí slándála i gcóras DCCG. Sainítear ann freisin cibé na heochracha agus na deimhnithe a úsáidtear chun cumarsáid, an fhaisnéis uaslódáilte, DCCanna agus liosta iontaoibhe sínithe de gach deimhniú CSCA ionduchtaithe a chosaint. Oibríonn DCCG mar mhol sonraí a éascaíonn malartú pacáistí sonraí sínithe le haghaidh na mBallstát.

Soláthraíonn DCCG na pacáistí sonraí uaslódáilte 'mar atá siad', rud a chiallaíonn nach gcuireann DCCG DSCanna leis na pacáistí a fhaigheann sé ná nó nach scríosann sé DSCanna ó na pacáistí a fhaigheann sé. Déanfar cúl náisiúnta (NB) na mBallstát a chumasú le sláine agus barántúlacht ó cheann go ceann na sonraí uaslódáilte a fhíorú. Thairis sin, úsáidfidh cúil náisiúnta agus DCCS fíordheimhniú frithpháirteach TLS chun nasc slán a bhunú. Tá sé sin sa bheith ar na sínithe sna sonraí malartaithe.

#### 3.1. Fíordheimhniú agus bunú naisc

Úsáideann DCCG Slándáil Shraith an Iompair (TLS) le fíordheimhniú frithpháirteach chun cainéal fíordheimhnithe criptithe a bhunú idir cúl náisiúnta (NB) an Bhallstáit agus timpeallacht na Tairsí. Dá bhrí sin, tá deimhniú freastalaí TLS i seilbh ag DCCG, a ghiorraítear mar DCCG<sub>TLS</sub>, agus tá deimhniú cliaint TLS i seilbh ag an gcúl náisiúnta – a ghiorraítear mar NB<sub>TLS</sub>. Soláthraítear teimpléid deimhnithe i *Roinn 5* Is féidir le gach cúl náisiúnta a dheimhniú TLS féin a sholáthar. Cuirfead an deimhniú sin ar gheall-liosta go sainráite agus dá réir sin féadfaidh údarás deimhniúcháin a bhfuil iontaoibh ag an bpobal as é a eisiúint (mar shampla, údarás deimhniúcháin a leanann ceanglais bhonnline an Fhóiraim Brabhsálaí CA), nó féadfaidh údarás náisiúnta deimhniúcháin é a eisiúint nó féadfaidh é a fhéinsíniú. Tá gach Ballstát freagrach as a chuid sonraí náisiúnta agus as an eochair phríobháideach a úsáidtear chun an nasc a bhunú le DCCG a chosaint. Éilítear próiseas clárúcháin agus aitheantais dea-shainithe leis an gcur chuige 'tabhair leat do dheimhniú féin' chomh maith le nósanna imeachta cúlghairme agus athnuachana ar a dtugtar tuairisc i *ranna 4.1, 4.2* agus *4.3*. Úsáideann DCCG geall-liosta i gcás ina gcuirtear deimhnithe TLS na gCúl Náisiúnta leo tar éis iad a chlárú go rathúil. Ní féidir ach le Cúl Náisiúnta a dhéanann iad féin a fhíordheimhniú le heochair phríobháideach a chomhfhreagraíonn do dheimhniú ón ngeall-liosta nasc slán a bhunú le DCCG. Bainfidh DCCG úsáid freisin as deimhniú TLS lena ligtear do Chúil Náisiúnta a fhíorú go bhfuil siad go deimhin ag bunú naisc leis an 'bhfíor'-DCCG agus ní le heintiteas éigin atá ag iarraidh díobháil a dhéanamh a ligeann air féin gur DCCG atá ann. Soláthrófar an deimhniú DCCG do na Cúl Náisiúnta tar éis clárú rathúil. Eiseofar an deimhniú DCCG<sub>TLS</sub> ó Údarás Deimhniúcháin a bhfuil iontaoibh ag an bpobal as (a chuimsítear i ngach mórbhrabhsálaí). Tá sé mar chúram ar na Ballstáit a fhíorú go bhfuil a nasc le DCCG slán (mar shampla, trí mhéarlorg deimhniú DCCG<sub>TLS</sub> an fhreastalaí a bhfuiltear nasctha leis a sheiceáil in aghaidh an ceann a soláthraíodh tar éis clárú).

#### 3.2. Údaráis Deimhniúcháin na Tíre Sínithe agus Samhail Bhailíochtaithe

Ní mór do na Ballstáit a bheidh páirteach sa chreat DCCG CSCA a úsáid chun DSCanna a eisiúint. Féadfaidh níos mó ná CSCA amháin a bheith ag na Ballstáit, i gcás dlárú réigiúnach, mar shampla. Is féidir le gach Ballstát údaráis deimhniúcháin atá ann cheana a úsáid nó is féidir leo údarás deimhniúcháin thiomnaithe (b'fhéidir féinsínithe) a bhunú le haghaidh an chórais DCC.



Ní mór do Bhallstáit a ndeimhniú/ndeimhnithe CSCA a thíolacadh don oibreoir DCCG i rith an nós imeachta ionductaithe oifigiúil. Tar éis an Ballstát a chlárú go rathúil (*féach roinn 4.1 chun tuilleadh sonraí a fháil*), tabharfaidh an t-oibreoir DCCG liosta iontaoibhe sínithe cothrom le dáta, liosta ina mbeidh gach deimhniú CSCA atá gníomhach sa chreat DCC. Úsáidfidh an t-oibreoir DCCG eochairphéire neamhshiméadrach tiomnaithe chun an liosta iontaoibhe agus na deimhnithe a shíniú i dtimpeallacht as líne. Ní stórálfar an eochair phríobháideach ar chóras ar líne DCCG, sa chaoi is má chuirtear an córas ar líne i mbaol nach gcuireann sé sin ar a chumas d'ionsaitheoir an liosta iontaoibhe a chur i mbaol. Soláthrófar an deimhniú cúltaca iontaoifa DCCG<sub>TA</sub> comhfhreagrach do na cúil náisiúnta i rith an phróisis ionductaithe.

Is féidir leis na Ballstáit an liosta iontaoibhe a aisghabháil ó DCCG le haghaidh a nósanna imeachta fíorúcháin. Sainítear CSCA mar an t-údarás deimhniúcháin a eisíonn DSCanna, mar sin ní mór do na Ballstáit a úsáideann ordlathas CA ilsraithe (mar shampla, Fréamh CA -> CSCA -> DSCanna) an t-údarás deimhniúcháin sóisearach a eisíonn DSCanna a sholáthar. Sa chás sin, má úsáideann Ballstát údarás deimhniúcháin atá ann cheana, ansin déanfaidh an córas DCC neamhaird d'aon rud os cionn CSCA agus ní chuirfidh siad ach CSCA ar an ngeal-liosta mar an cúltaca iontaoibhe (cé gur údarás deimhniúcháin sóisearach é). Tá sé sin cosúil leis an tsamhail ICAO, nach gceadaíonn ach díreach dhá leibhéal – ‘fréamh’-CSCA agus DSC le ‘duille’ a shíníonn an CSCA sin amháin.

I gcás ina n-oibríonn Ballstát a CSCA féin, tá an Ballstát freagrach as oibriocht shlán agus as príomhbhainistíocht an údaráis deimhniúcháin sin. Bíonn CSCA mar chúltaca iontaoifa do DSCanna, agus dá bhrí sin tá sé fíor-riachtanach go dtabharfaí cosaint d'eochair phríobháideach CSCA ar mhaithe le sláine na timpeallachta DCC. Is í an tsamhail fíorúcháin in PKI de chuid DCC an tsamhail bhlaoise, ina luaitear nach mór do gach deimhniú i mbailíochtú an chosáin deimhnithe a bheith bailí ag tráth ar leith (i.e. tráth bhailíochtú an tsínithe). Dá bhrí sin, beidh feidhm ag na srianta seo a leanas:

- Ní eiseoidh CSCA deimhnithe a bheidh bailí níos faide ná an deimhniú CA féin;
- Ní shíneoidh an sínitheoir doiciméad doiciméid a bheidh bailí níos faide ná DSC féin;
- Ní mór do na Ballstáit a oibríonn a CSCA féin tréimhsí bailíochta a shainiú dá CSCA agus gach deimhniú a eiseofar agus ní mór dóibh cúram a ghlacadh as athnuachan na ndeimhnithe.

Tá moltaí i *roinn 4.2* maidir le tréimhsí bailíochta.

### 3.3. Sláine agus barántúlacht na sonraí a uaslódálfar

Is féidir leis na cúil náisiúnta DCCG a úsáid chun pacáistí sonraí atá sínithe go leictreonach a uaslódáil agus a íoslódáil tar éis fíordheimhniú rathúil frithpháirteach. Bíonn DSCanna na mBallstát sna pacáistí sonraí sin ar dtús báire. An t-eochairphéire a úsáideann an cúl náisiúnta le haghaidh shíniú leictreonach na bpacáistí sonraí a uaslódáiltear sa chóras DCCG, tugtar eochairphéire sínithe i gcomhair uaslódála chuig an gcúl náisiúnta ar an eochairphéire sin agus giorraítear an deimhniú eochrach poiblí comhfhreagrach le deimhniú NB<sub>UP</sub>. Tugann gach Ballstát a dheimhniú NB<sub>UP</sub> féin leis, ar féidir leis féin é a shíniú, nó is féidir le húdarás deimhniúcháin atá i bhfeidhm cheana é a eisiúint, amhail údarás deimhniúcháin poiblí (i.e. údarás deimhniúcháin a eisíonn deimhniú i gcomhréir le ceanglais bhonnlíne Fhóram CAB). Beidh an deimhniú NB<sub>UP</sub> difriúil le haon deimhniú eile a bhíonn á úsáid ag an mBallstát (i.e. CSCA, cliant TLS nó DSCanna).

Ní mór do na Ballstáit an deimhniú uaslódála a sholáthar don oibreoir DCCG i rith an nós imeachta clárúcháin tosaigh (*féach Roinn 4.1 chun tuilleadh sonraí a fháil*). Tá gach Ballstát freagrach as a shonraí náisiúnta agus ní mór dó cosaint a thabhairt don eochair phoiblí a úsáidtear chun na huaslódálacha a shíniú.

Is féidir leis na Ballstáit eile na pacáistí sonraí sínithe a fhíorú ag úsáid na ndeimhnithe uaslódála a sholáthraíonn DCCG. Fíoraíonn DCCG barántúlacht agus sláine na sonraí uaslódáilte leis an deimhniú uaslódála NB sula soláthraítear iad do na Ballstáit eile.

### 3.4. Ceanglais maidir le hailtireacht theicniúil DCCG

Is mar a leanas atá na ceanglais maidir le hailtireacht theicniúil DCCG:

- Úsáideann DCCG fíorúchán TLS frithpháirteach chun nasc criptithe fíordheimhnithe a bhunú leis na Cúil Náisiúnta. Dá bhrí sin, coinníonn DCCG geal-liosta de dheimhnithe cliant NB<sub>TLS</sub> cláraithe;
- Úsáideann DCCG dhá dheimhniú dhigiteacha (DCCG<sub>TLS</sub> agus DCCG<sub>TA</sub>) a bhfuil dhá eochairphéire ar leith ag gabháil leo. Coinnítear eochair phríobháideach eochairphéire DCCG<sub>TA</sub> as líne (ní ar na comhpháirteanna ar líne de DCCG);

- Coinníonn DCCG liosta iontaoibhe de dheimhnithe  $NB_{CSCA}$  atá sínithe le heochair phríobháideach  $DCCG_{TA}$ ;
- Ní mór do na sífir a úsáidtear na ceanglais ó *Roinn 5.1* a chomhlíonadh.

#### 4. Bainistíocht Shaolré an Deimhnithe

##### 4.1. Clárú na gCúl Náisiúnta

Ní mór do na Ballstáit clárú leis an oibreoir DCCG chun a bheith páirteach sa chóras DCCG. Tugtar tuairisc sa roinn seo ar an nós imeachta teicniúil agus oibríochta nach mór a chomhlíonadh chun cúl náisiúnta a chlárú.

Ní mór don oibreoir DCCG agus don Bhallstát faisnéis a mhalartú faoi theagmhálaithe teicniúla don phróiseas ionductaithe. Glactar leis go bhfuil na teagmhálaithe teicniúla dlisteanaithe ag a mBallstáit agus go ndéantar aitheantas/fíordheimhniú ar chainéil eile. Mar shampla, is féidir fíordheimhniú a bhaint amach nuair a sholáthraíonn teagmhálaí teicniúil Ballstáit na deimhnithe mar chomhaid atá criptithe le pasfhocal trí ríomhphost agus nuair a chomhroinneann sé an pasfhocal comhfhreagrach leis an oibreoir DCCG ar an teileafón. Féadfar cainéil shlána eile a bheidh sainithe ag an oibreoir DCCG a úsáid freisin.

Ní mór don Bhallstát trí dheimhniú dhigiteacha a sholáthar i rith an phróisis clárúcháin agus aitheantais:

- Deimhniú TLS  $NB_{TLS}$  an Bhallstáit
- Deimhniú uaslódála  $NB_{UP}$  an Bhallstáit
- Deimhniú/deimhnithe  $CSCA$   $NB_{CSCA}$  an Bhallstáit

Ní mór do gach deimhniú a sholáthraítear cloí leis na ceanglais a shainítear i *Roinn 5*. Fíoróidh an t-oibreoir DCCG go gcloíonn an deimhniú a sholáthraítear le ceanglais *Roinn 5*. Tar éis an aitheantais agus an chlárúcháin, déanfaidh an t-oibreoir DCCG na nithe a leanas:

- cuirfidh sé an deimhniú/na deimhnithe  $NB_{CSCA}$  leis an liosta iontaoibhe arna shíniú leis an eochair phríobháideach a chomhfhreagraíonn don eochair phoiblí  $DCCG_{TA}$ ;
- cuirfidh sé an deimhniú  $NB_{TLS}$  leis an ngeal-liosta de chríochphointe DCCG TLS;
- cuirfidh sé an deimhniú  $NB_{UP}$  leis an gcóras DCCG;
- soláthróidh sé an deimhniú eochrach poiblí  $DCCG_{TA}$  agus  $DCCG_{TLS}$  don Bhallstát.

##### 4.2. Údarais deimhniúcháin, tréimhsí bailíochta agus athnuachan

I gcás inar mian le Ballstát  $CSCA$  dá chuid féin a oibriú, is féidir leis na deimhnithe  $CSCA$  a bheith ina ndeimhnithe féinsínithe. Feidhmíonn siad mar chúltaca iontaofa de chuid an Bhallstáit agus dá bhrí sin ní mór don Bhallstát an eochair phríobháideach a chomhfhreagraíonn d'eochair phoiblí an deimhnithe  $CSCA$  a chosaint go láidir. Moltar go n-úsáidfeadh na Ballstáit córas as líne dá  $CSCA$ , i.e. córas ríomhairí nach bhfuil nasctha le haon líonra. Úsáidfear rialúcháin ildaoine chun an córas a rochtain (mar shampla, ag leanúint phrionsabal na gceithre shúil). Tar éis DSCanna a shíniú, cuirfear rialúcháin oibríochtúla i bhfeidhm agus déanfar an córas ina gcoinnítear an eochair phríobháideach  $CSCA$  a stóráil go sábháilte le rialúcháin rochtana láidre. Is féidir Modúil Shlándála Chrua-earraí nó Cáirtaí Cliste a úsáid chun cosaint bhreise a thabhairt don eochair phríobháideach  $CSCA$ . Tá tréimhse bhailíochta ag gabháil leis na deimhnithe digiteacha a fhorfheidhmíonn athnuachan an deimhnithe. Is gá athnuachan a dhéanamh chun eochracha cripteagrafacha as an nua a úsáid agus chun méideanna eochrach a oiriúnú nuair a chuireann feabhsúcháin nua sa ríomhaireacht nó ionsaithe nua slándáil an algartaim chripteagrafaigh a úsáidtear i mbaol. Beidh feidhm leis an tsamhail bhlaoisce (féach *Roinn 3.2*).

Moltar na tréimhsí bailíochta seo a leanas, ag glacadh le bailíocht bliana le haghaidh na ndeimhnithe digiteacha COVID:

- $CSCA$ : 4 bliana
- DSC: 2 bhliain
- Uaslódáil: 1–2 bhliain
- Fíordheimhniú Cliant TLS: 1–2 bhliain

Ar mhaithe le hathnuachan thráthúil, moltar na tréimhsí úsáide seo a leanas le haghaidh na n-eochracha príobháideacha:

- $CSCA$ : 1 bhliain
- DSC: 6 mhí

Ní mór do na Ballstáit deimhnithe nua uaslódála agus deimhnithe TLS a chruthú go tráthúil, mar shampla, mí amháin, roimh dóibh dul in éag d'fhonn oibríocht chomhréidh a cheadú. Ba cheart deimhnithe CSCA agus DSCanna a athnuachan mí amháin ar a laghad sula dtagann deireadh le húsáid na heochrach príobháidí (ag cur na nósanna imeachta oibríochta is gá san áireamh). Ní mór do na Ballstáit deimhnithe CSCA, uaslódála agus TLS cothrom le dáta a sholáthar don oibreoir DCCG. Bainfear deimhnithe éagtha ón ngeal-liosta agus ón liosta iontaoibhe.

Ní mór do na Ballstáit agus don oibreoir DCCG súil a choimeád ar bhailíocht a ndeimhnithe féin. Níl aon eintiteas lárnach a choimeádann taifead ar bhailíocht na ndeimhnithe agus a chuireann na rannpháirtithe ar an eolas.

#### 4.3. Deimhnithe a chúlghairm

Go ginearálta, is féidir lena CA eisiúna na deimhnithe digiteacha a chúlghairm trí úsáid a bhaint as liostaí cúlghairme deimhnithe nó Freagróir Prótacail Stádais Deimhniúcháin Ar Líne (OCSP). Ba cheart do CSCanna le haghaidh an chórais DCC liostaí cúlghairme deimhnithe (CRLanna) a sholáthar. Fiú mura n-úsáideann Ballstáit eile na CRLanna sin, ba cheart iad a chomhtháthú lena gcur i bhfeidhm sa todhchaí. I gcás ina gcinneann CSCA gan CRLanna a sholáthar, ní mór na DSCanna de chuid CSCA mar sin a athnuachan nuair a éireoidh CRLanna éigeantach. Níor cheart d'fhóraitheoirí OCSP a úsáid chun DSCanna a fhóirú agus ba cheart dóibh CRLanna a úsáid. Moltar go ndéanadh an cúl náisiúnta an bailíochtú is gá ar DSCanna a uaslódáiltear ón Tairseach DCC agus nach gcuirfí ach tacar DSC iontaofa agus bailíochtaithe ar aghaidh chuig bailíochtóirí náisiúnta DCC. Níor cheart do bhailíochtóirí DCC aon seiceáil aisghairme a dhéanamh ar DSC ina bpróiseas bailíochtaithe. Cúis amháin atá leis sin is ea chun príobháideachas sealbhóirí DCC a chosaint trí aon seans gur féidir le freagróir OCSP comhlachaithe faireachán a dhéanamh ar úsáid aon DSC ar leith a sheachaint.

Is féidir leis na Ballstáit a DSCanna a bhaint óna DCCG as a stuaim féin ag úsáid deimhnithe uaslódála agus TLS bailí. Nuair a bhaintear DSC ciallaíonn sé sin go n-éireoidh gach DCC a eisíodh leis an DSC sin neamhbhailí nuair a gheobhaidh na Ballstáit na liostaí DSC atá tugtha cothrom le dáta. Tá sé rithabhachtach go dtabharfaí cosaint don ábhar atá sna heochracha príobháideacha a chomhfhreagraíonn do DSCanna. Ní mór do na Ballstáit an t-oibreoir DCCG a chur ar an eolas nuair a chaithfidh siad deimhnithe uaslódála nó TLS a chúlghairm, i ngeall ar an gcúl náisiúnta a chur i mbaol, mar shampla. Is féidir leis an oibreoir DCCG an iontaoibh don deimhniú dá ndéantar difear a bhaint ansin, trína bhaint ón ngeal-liosta TLS, mar shampla. Is féidir leis an oibreoir DCCG na deimhnithe uaslódála a bhaint as an mbunachar sonraí DCCG. Beidh pacáistí arna síniú leis an eochair phríobháideach a chomhfhreagraíonn don deimhniú uaslódála sin neamhbhailí nuair a bhainfidh cúl náisiúnta iontaoibh an deimhnithe uaslódála aisghairme. I gcás nach mór deimhniú CSCA a chúlghairm, cuirfidh na Ballstáit an t-oibreoir DCCG ar an eolas chomh maith leis na Ballstáit eile a bhfuil caidrimh iontaoibhe acu leo. Éireoidh an t-oibreoir DCCG liosta nua iontaoibhe i gcás nach bhfuil an deimhniú dá ndearnadh difear ann níos mó. Éireoidh gach DSC arna n-eisiúint ag CSCA mar sin neamhbhailí nuair a thabharfaidh Ballstáit stór iontaofa a gcúl náisiúnta cothrom le dáta. I gcás nach mór an deimhniú DCCG<sub>TLS</sub> nó an deimhniú DCCG<sub>TA</sub> a chúlghairm, ní mór don oibreoir DCCG agus do na Ballstáit oibriú le chéile chun nasc nua iontaofa TLS agus liosta iontaoibhe nua a bhunú.

## 5. Teimpléid Deimhnithe

Leagtar amach ceanglais chripteagrafacha agus treoraíocht sa roinn seo chomh maith le ceanglais maidir le teimpléid deimhnithe. Le haghaidh na ndeimhnithe DCCG, sainmhínítear na teimpléid deimhnithe sa roinn seo.

### 5.1. Ceanglais chripteagrafacha

Déanfar algartaim chripteagrafacha agus svúiteanna sífir TLS a roghnú bunaithe ar an moladh reatha ó Oifig Fheidearálach na Gearmáine um Shlándáil Faisnéise (BSI) nó SOG-IS. Tá na moltaí sin agus moltaí institiúidí eile agus eagraíochta caighdeánaithe cosúil lena chéile. Is féidir na moltaí a fháil sna treoirlínte teicniúla TR 02102-1 agus TR 02102-2 <sup>(1)</sup> nó Sársaí Cripteagrafacha Comhaontaithe SOG-IS <sup>(2)</sup>.

#### 5.1.1. Ceanglais maidir le DSC

Beidh feidhm ag na ceanglais dá bhforáiltear in *Iarscríbhinn I, Roinn 3.2.2*. Dá bhrí sin, moltar go láidir go n-úsáidfídh Síntheoirí Doiciméad Algartam Sínthe Dhigitigh Cuair Éilipsigh (ECDSA) le NIST-p-256 (mar a shainmhínítear in Auisín D de FIPS PUB 186-4). Ní thacaítear le cuair éilipseacha eile. Mar gheall ar shrianta spáis DCC, níor cheart

<sup>(1)</sup> BSI – Treoirlínte Teicniúla TR-02102 (bund.de)

<sup>(2)</sup> SOG-IS - Doiciméid tacaíochta (sogis.eu)

do Bhallstáit RSA-PSS a úsáid, fiú má cheadaítear é mar algartam cúltaca. I gcás ina n-úsáideann Ballstáit RSA-PSS, ba cheart dóibh modal de mhéid 2048 nó uasmhéid de 3072 ghiotán a úsáid. Úsáidfear SHA-2 a bhfuil fad aschuir  $\geq 256$  ghiotán aige mar haisfheidhm chripteagrafach (féach ISO/IEC 10118-3:2004) don síniú DSC.

### 5.1.2. Ceanglais maidir le deimhnithe TLS, Uaslódáil agus CSCA

Maidir le deimhnithe digiteacha agus sínithe cripteagrafacha i gcomhthéacs DCCG, tugtar achoimre ar na príomhriachtanais maidir le halgartaim chripteagrafacha agus fad eochrach sa tábla seo a leanas (amhail ó 2021):

| Algartam Sínithe                                             | Méid eochrach                                                           | Haisfheidhm                             |
|--------------------------------------------------------------|-------------------------------------------------------------------------|-----------------------------------------|
| EC-DSA                                                       | Íosmhéid de 250 Giotán                                                  | SHA-2 le fad aschuir $\geq 256$ Ghiotán |
| RSA-PSS (stuáil mholta) RSA-PKCS#1 v1.5 (stuáil oidhreachta) | Modal RSA 3000 Giotán ar a laghad (N) le heaspónant poiblí $e > 2^{16}$ | SHA-2 le fad aschuir $\geq 256$ Ghiotán |
| DSA                                                          | P príomha 3000 Giotán ar a laghad, eochair q 250 Giotán                 | SHA-2 le fad aschuir $\geq 256$ Ghiotán |

Is é NIST-p-256 an cuar éilipseach a mholtar le haghaidh EC-DSA toisc go gcuirtear i bhfeidhm é go forleathan.

### 5.2. Deimhniú CSCA ( $NB_{CSCA}$ )

Tugtar treoraíocht sa tábla seo a leanas maidir le teimpléad an deimhnithe  $NB_{CSCA}$  má chinneann Ballstát CSCA dá chuid féin a fheidhmiú don chóras DCC.

Éilítear iontrálacha i gcló **trom** (ní mór iad a chur san áireamh sa deimhniú), moltar iontrálacha i gcló *iodálach* (ba cheart iad a chur san áireamh). Ní shainítear aon mholtaí maidir le réimsí atá in easnamh.

| Réimse                   | Luach                                                                                                                |
|--------------------------|----------------------------------------------------------------------------------------------------------------------|
| <b>Ábhar</b>             | <b>cn=&lt;ainm coitianta uathúil agus neamhfholamh&gt;,o=&lt;Soláthraí&gt;,c=&lt;An Ballstát a oibríonn CSCA&gt;</b> |
| <b>Úsáid eochrach</b>    | <b>síniú deimhnithe,síniú CRL (ar a laghad)</b>                                                                      |
| <b>Srianta Bunúsacha</b> | <b>CA = fíorshrianta ar fhad cosáin = 0</b>                                                                          |

Ní féidir le hainm an ábhair a bheith folamh agus ní mór é a bheith uathúil laistigh den Bhallstát a shonraítear. Ní mór don chód tíre (c) a bheith ar aon dul leis an mBallstát a úsáidfídh an deimhniú CSCA sin. Ní mór aitheantóir eochrach ábhair (SKI) uathúil a bheith sa deimhniú, de réir RFC 5280 <sup>(3)</sup>.

### 5.3. Deimhniú Sínteora Doiciméad (DSC)

Soláthraítear treoraíocht sa tábla seo a leanas maidir leis an DSC. Éilítear iontrálacha i gcló **trom** (ní mór iad a chur san áireamh sa deimhniú), moltar iontrálacha i gcló *iodálach* (ba cheart iad a chur san áireamh). Ní shainítear aon mholtaí maidir le réimsí atá in easnamh.

| Réimse                | Luach                                                                                                                        |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------|
| <b>Sraithuimhir</b>   | <b>sraithuimhir uathúil</b>                                                                                                  |
| <b>Ábhar</b>          | <b>cn=&lt;ainm coitianta uathúil agus neamhfholamh&gt;,o=&lt;Soláthraí&gt;,c=&lt;An Ballstát a úsáideann DSC mar seo&gt;</b> |
| <b>Úsáid Eochrach</b> | <b>síniú digiteach (ar a laghad)</b>                                                                                         |

<sup>(3)</sup> rfc5280 (ietf.org)

Ní mór DSC a shíniú leis an eochair phearsanta a chomhfhreagraíonn do dheimhniú CSCA a úsáideann an Ballstát.

Ní mór na breisithe seo a leanas a úsáid:

- Ní mór Aitheantóir Eochrach Údaráis (AKI) a bheith sa deimhniú, a mheaitseálann Aitheantóir Eochrach Ábhair (SKI) an deimhnithe CSCA eisiúna
- Ba cheart Aitheantóir Eochrach Ábhair uathúil a bheith sa deimhniú (i gcomhréir le RFC 5280 <sup>(4)</sup>)

Sa bhreis air sin, ba cheart breisiú an phointe dáilte CRL a bheith san áireamh sa deimhniú, lena léirítear an liosta cúlghairme deimhnithe (CRL) a sholáthraíonn CSCA a d'eisigh DSC.

Féadfaidh breisiú úsáide eochrach sínte a bheith in DSC le haitheantóirí beartais úsáide eochrach nialasacha, nó níos mó ná sin, a chuireann srianadh ar na cineálacha HCERTanna a cheadaítear don deimhniú sin a fhíorú. Má tá ceann amháin nó níos mó ann, déanfaidh na fíoraitheoirí úsáid eochrach a fhíorú in aghaidh HCERT stóráilte. Sainmhínítear na luachanna ÚsáidEochrachshínte seo a leanas ina leith sin:

| Réimse              | Luach                                                         |
|---------------------|---------------------------------------------------------------|
| ÚsáidEochrachshínte | 1.3.6.1.4.1.1847.2021.1.1 le haghaidh Eisitheoirí Tástála     |
| ÚsáidEochrachshínte | 1.3.6.1.4.1.1847.2021.1.2 le haghaidh Eisitheoirí Vacsaínithe |
| ÚsáidEochrachshínte | 1.3.6.1.4.1.1847.2021.1.3 le haghaidh Eisitheoirí Téarnaimh   |

In éagmais aon bhreisithe úsáide eochrach (i.e. gan aon bhreisithe nó le breisithe nialasacha), féadfar an deimhniú sin a úsáid chun aon chineál HCERT a bhailíochtú. Féadfar sainmhíniú a sholáthar i ndoiciméid eile ar aitheantóirí beartais úsáide eochrach sínte breise ábhartha a úsáidtear maidir le HCERTanna a bhailíochtú.

#### 5.4. Deimhnithe Uaslódála (NBUP)

Soláthraítear treoraíocht sa tábla seo a leanas maidir leis an deimhniú uaslódála cúil náisiúnta. Éilítear iontrálacha i gcló **trom** (ní mór iad a chur san áireamh sa deimhniú), moltar iontrálacha i gcló *iodálach* (ba cheart iad a chur san áireamh). Ní shainítear aon mholtaí maidir le réimsí atá in easnamh.

| Réimse                | Luach                                                                                                                                       |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Ábhar</b>          | <b>cn=&lt;ainm coitianta uathúil agus neamhfholamh&gt;, o=&lt;Soláthraí&gt;,c=&lt;An Ballstát a úsáideann an deimhniú uaslódála seo&gt;</b> |
| <b>Úsáid Eochrach</b> | <b>síniú digiteach</b> (ar a laghad)                                                                                                        |

#### 5.5. Fíordheimhniú Cliaint TLS Cúil Náisiúnta (NB<sub>TLS</sub>)

Soláthraítear treoraíocht sa tábla seo a leanas maidir leis an deimhniú um fhíordheimhniú cliaint TLS cúil náisiúnta. Éilítear iontrálacha i gcló **trom** (ní mór iad a chur san áireamh sa deimhniú), moltar iontrálacha i gcló *iodálach* (ba cheart iad a chur san áireamh). Ní shainítear aon mholtaí maidir le réimsí atá in easnamh.

| Réimse                       | Luach                                                                                                                      |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| <b>Ábhar</b>                 | <b>cn=&lt;ainm coitianta uathúil agus neamhfholamh&gt;, o=&lt;Soláthraí&gt;,c=&lt;An Ballstát ar an gcúl náisiúnta&gt;</b> |
| <b>Úsáid Eochrach</b>        | <b>síniú digiteach</b> (ar a laghad)                                                                                       |
| <b>Úsáid eochrach shínte</b> | <b>fíordheimhniú cliaint (1.3.6.1.5.5.7.3.2)</b>                                                                           |

<sup>(4)</sup> rfc5280 (ietf.org)

Féadfaidh an *fiordheimhniú freastalaí um úsáid eochrach shínte* (1.3.6.1.5.5.7.3.1) a bheith sa deimhniú freisin, ach ní éilítear é.

5.6. *Deimhniú sínithe an liosta iontaoibhe (DCCG<sub>TA</sub>)*

Sainmhínítear deimhniú an Chúltaca Iontaoibhe DCCG sa tábla seo a leanas.

| Réimse                | Luach                                                                                                        |
|-----------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Ábhar</b>          | <b>cn = Tairseach na nDeimhnithe Glasa Digiteacha <sup>(5)</sup>,<br/>o=&lt;Soláthraí&gt;, c=&lt;tír&gt;</b> |
| <b>Úsáid Eochrach</b> | <b>síniú digiteach</b> (ar a laghad)                                                                         |

5.7. *Deimhnithe Freastalaí DCCG TLS (DCCG<sub>TLS</sub>)*

Sainmhínítear an deimhniú DCCG TLS sa tábla seo a leanas.

| Réimse                       | Luach                                                                         |
|------------------------------|-------------------------------------------------------------------------------|
| <b>Ábhar</b>                 | <b>cn=&lt;FQDN nó seoladh IP DCCG&gt;, o=&lt;Soláthraí&gt;, c=&lt;tír&gt;</b> |
| <b>AinmMalartachÁbhair</b>   | <b>dNSAinm: &lt;Ainm DNS DCCG&gt; nó SeoladhIP: &lt;Seoladh IP DCCG&gt;</b>   |
| <b>Úsáid Eochrach</b>        | <b>síniú digiteach</b> (ar a laghad)                                          |
| <b>Úsáid Eochrach shínte</b> | <b>fiordheimhniú freastalaí (1.3.6.1.5.5.7.3.1)</b>                           |

Féadfaidh an *fiordheimhniú cliaint um úsáid eochrach shínte* (1.3.6.1.5.5.7.3.2) a bheith sa deimhniú freisin, ach ní éilítear é.

Eiseoidh údarás deimhniúcháin a bhfuil iontaoibh ag an bpobal as deimhniú DCCG TLS (a chuimsítear i ngach mórbhrabhsálaí agus córas oibriúcháin, de réir cheanglais bhunaidh Fhóram CAB).

<sup>(5)</sup> Coinníodh an téarmaolaíocht 'Deimhniú Glas Digiteach' seachas 'Deimhniú Digiteach COVID AE' ar bun sa chomhthéacs seo ós rud é gurb é sin an téarmaolaíocht ar a ndearnadh cruachódú agus a cuireadh i bhfeidhm sa deimhniú sular chinn na comhreachtóirí téarmaolaíocht nua a úsáid.